车联网隐私保护研究综述 *

邓雨康，张 磊，李 晶†

(佳木斯大学 信息电子技术学院，黑龙江 佳木斯 154007)

摘 要：随着私有车辆的与日俱增，人们迫切需要一个安全、舒适、便利的交通环境。车联网是一种通过在车辆、行人、路边单元等通信实体之间构建一个网络拓扑来提供高效、安全的信息服务的网络。车联网能够有效满足人们对交通环境日益增长的需求，但由于车联网具有移动性和开放性的特点，因此容易遭受攻击。在众多的威胁中，车联网用户的隐私泄露，可能会造成不可弥补的损失，因此车联网的隐私保护被研究者广泛关注。针对车联网的隐私保护问题展开研究，根据车联网的体系结构总结出车联网需要具备的四个基本性质，并对现有的车联网攻击模型加以分析。通过对近些年车联网隐私保护方案的调查总结，对现有研究中常用的方法加以归类。然后将车联网的隐私保护研究依照保护对象分为三类，并对各方案进行了分析评价。同时，对现有研究的看法和面临的挑战进行了总结。最后对全文进行了总结，并给出了对未来研究的展望。

关键词：车联网；隐私保护；体系结构；攻击方法

中图分类号：TP391 doi: 10.19734/j.issn.1001-3695.2022.02.0091

Overview of research on privacy protection of Internet of Vehicles

Deng Yukang, Zhang Lei, Li Jing†

(*School of Information & Electronic Technology*, *Jiamusi University*, *Jiamusi Heilongjiang* 154007, *China*)

Abstract: With the increasing number of private vehicles, people urgently need a safe, comfortable and convenient transportation environment. Internet of vehicles is a network that provides efficient and safe information services by building a network topology among communication entities such as vehicles, pedestrians and roadside units. The Internet of vehicles can effectively meet people's growing demand for the traffic environment, but it is vulnerable to attack because of its mobility and openness. Among many threats, the privacy disclosure of Internet of vehicles users may cause irreparable losses. Therefore, the privacy protection of Internet of vehicles has been widely concerned by researchers. This paper studies the privacy protection of the Internet of vehicles, summarizes the four basic properties of the Internet of vehicles according to the architecture of the Internet of vehicles, and analyzes the existing Internet of vehicles attack model. Through the investigation and summary of the privacy protection schemes of the Internet of vehicles in recent years, the methods commonly used in the existing research are classified. Then, the research on privacy protection of Internet of vehicles is divided into three categories according to the protection objects, and each scheme is analyzed and evaluated. At the same time, the views and challenges of the existing research are summarized. Finally, the full text is summarized and the prospect of future research is given.

Key words: Internet of Vehicles; privacy protection; architecture; attack method

chinaXiv:202205.00140v1

0 引言

截止 2017 年，中国汽车的累计生产量和销售量分别为 2572.1 万辆和 2576.9 万辆[1]。根据文献[2]的预测，到 2022 年，联网汽车市场将再增长 270%，全球汽车总量将超过 1.25 亿辆。经济和人口的增长导致了车辆数量的增加，大规模增长的车辆给道路交通带来了许多问题，包括交通事故、交通拥堵、违规停车等。根据世界卫生组织(World Health Organization, WTO)的一份医疗健康报告[3]，15-29 岁人群死亡的主要原因是交通事故，全球每年也有 130 万人死于交通事故。交通事故发生率的快速增长可以通过使用最新的技术，向驾驶员实时报告车辆安全参数、道路状况、交通堵塞情况和天气预警来缓解。除了为驾驶员提供安全的驾驶环境，人们也开始重视提高驾驶环境的舒适性，更多信息交互的交通服务应运而生，一种称为车联网(Internet of Vehicle, IoV)的新兴范式也被提出来助力智慧交通系统(Intelligent Transport System, ITS)的发展[4]。车联网具有强大的实时车辆信息收集能力[5]，在帮助避免交通事故[6]、缓解交通拥堵[7]、提供多样化服务[8]方面发挥了重要作用[9]。

根据文献[10]的预测，到 2023 年全球 70%的轻型车辆和轨道将连接到互联网，面对来势汹汹的汽车热潮和高速发展的无线传感技术，车联网这一新兴范式迎来了更为广泛的关注。而真正将车联网应用到实际生活中还需要解决车联网本身的限制，主要有两方面的限制：一个是安全性，另一个是可用性。本文主要研究车联网中的隐私保护问题，通过调查总结出车联网应该具备的四项基本性质，分别为权衡性、适应性、可靠性和完备性，在此基础上研究了近些年车联网中的隐私安全问题，以及学者们对不同的安全问题采用的不同解决方案，在这些方案中存在的不足以及这些方案本身的特点。通过比较研究，对车联网中现有的隐私保护方案进行了分类，还提出了一系列的评估标准，根据所提出的标准分析评估了现有的隐私保护方案的性能，发现了一些开放性的隐私保护挑战，为车联网隐私保护未来的研究提供帮助。本文的主要贡献如下：

收稿日期：2022-02-13；**修回日期：**2022-03-29 **基金项目：**黑龙江省省属高等学校基本科研业务费项目优秀创新团队项目(2019-KYYWF-1335)；佳木斯大学优秀学科团队项目(JDXKTDG2019008)；黑龙江省自然科学基金资助项目(LH2021F054)

作者简介：邓雨康(1999-)，男，江西南昌人，硕士研究生，主要研究方向为车联网、隐私保护；张磊(1982-)，男，黑龙江绥化人，教授，博士，主要研究方向为信息安全、隐私保护；李晶(1968-)，女(通信作者)，黑龙江人，教授，硕士，主要研究方向为数据挖掘、信息安全(lijing2483@163.com).

ChinaXiv合作期刊

• 详细地总结出车联网应该具备的四个基本性质；

• 介绍现有的车联网攻击方式和隐私保护方法；

• 以本文总结的四个基本性质作为评价指标分析了一些现有研究，然后对比研究了近些年车联网隐私保护研究的现状；

• 提出车联网隐私保护中面临的挑战和对未来的展望。

本文的后续结构可简单划分为如下几个部分，第 1 章节介绍 IoV 的体系结构并在此基础上总结车联网应该具备的四个基本性质，然后总结了 IoV 现存的攻击方式。第 2 章中分类介绍一些最新的车联网隐私保护方法。本文的第 3 章节对这些隐私保护方案进行了对比分析并提出了一些开放性挑战。最后，第 4 章是对本文的总结和对未来车联网隐私保护的展望。

1　车联网的架构、性质与安全隐患

在本章节本文介绍了车联网的体系结构并根据调查总结出车联网应具备的四个基本性质，然后在此基础上介绍了如今车联网可能遭受到的攻击方式和存在的安全隐患。

1.1　车联网的架构

1.1.1　车联网(IoV)与车载自组织网络(Vehicular Ad hoc Networks, VANETs)

经过本文的调查研究发现，车联网(IoV)与车载自组织网络(VANETs)在学术界没有十分严格的区分，有一些文章将车载自组织网络称为车联网[11, 12]，还有一些文章还将车联网称为车载网络(Vehicular Network, VN)[13, 14]。但实际上它们之间还是有明显区别的，车载自组织网络是起源于移动自组织网络(Mobile Ad hoc Networks, MANETs)[15, 16]，主要目的是研究车辆的移动性管理、广播和路由协议等通信领域的范畴。而车联网被认为是物联网(Internet of Things, IoT)[17]的一种独特应用。实际上，车联网是物联网与车载自组织网络的结合应用[18, 19]，是智慧交通系统(ITS)提出以后，将通信领域、车辆传感、边缘计算或云计算等技术相结合提出的新概念，适用的范围更广，能够提供的服务也更加全面。车载网络(VN)则从属于车联网(IoV)三层体系中的网络层[20]，在本文的 1.1.2 节将会详细介绍车联网的三层架构。在学术研究中三者往往会互相使用，但本文将 IoV 与 VANETs 作出区分，在本文中 IoV 被认为是 VANETs[21]的超集，它扩展了 VANETs 的规模、应用和结构。它强调了来自车辆、路边单元(Road Side Unit, RSU)和人类用户的信息交互作用。它还旨在为人们提供低延迟的道路交通信息，以确保他们驾驶的安全性和舒适性。与 VANETs 相比，车联网将车辆作为拥有多个传感器的智能载体，并连接到互联网，具有一定的计算和存储能力[22]，还具备能够满足用户需求的学习能力[23]。

1.1.2 整体架构

车联网整体上可以划分为三层，即：感知层、网络层和应用层[24, 25]。车联网的三层架构也有一些其他的叫法，例如文献[26]中将车联网的三层架构分为：车载端、通信层和云管层。车联网的三层模型是认可度最为广泛的，除此之外也有研究提出了四层模型[27]、五层模型[28]、六层模型[29]和七层模型[30]，这些模型在三层模型的基础之上进一步细化，因而分成了更多的层次，但三层的模型有着广泛的研究基础，在形式上也足以描述车联网的整体结构，因此在本文的研究中，本文依照感知层、网络层、应用层这三层模型来展开介绍车联网的架构，如图 1 所示。

a) 感知层。感知层被称作车联网的“神经末梢”，通过射频识别(Radio Frequency Identification, RFID)[31]、全球定位系统(Global Positioning System, GPS)、北斗定位系统、车载雷达、车载摄像头、车载娱乐设施等车载传感器和道路监控、路边单元等交通基础设施的协同感知，将收集到的车内外行驶状态信息、交通状况信息和道路环境信息反馈给驾驶员，驾驶员根据收到的反馈信息作出行驶决策，实现感知数据辅助驾驶的功能[32]。感知层一方面通过传感器采集车辆、道路、环境以及驾驶员信息，另一方面也为驾驶员提供娱乐、行车安全以及交通环境监测识别等服务，是智能驾驶决策、智能交通管控、车载信息服务等车联网服务的基础[26]。将感知层中传感器接收到的车辆数据上传到网络层中，可以为行车人员提供一个更加安全舒适的驾驶环境。图 2 给出了感知层的各部分模块，同时介绍了感知层中车载设备之间的联系。

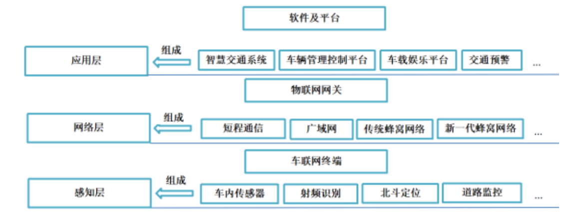


图 1　车联网的三层架构

Fig. 1　Three-layer architecture of IoV

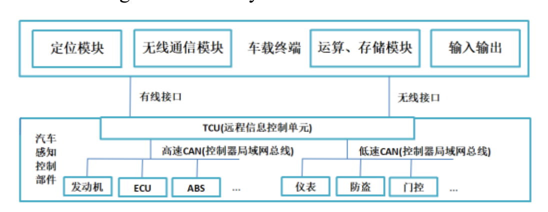


图 2　感知层模型

Fig. 2　Perception layer model

b) 网络层。网络层主要通过车载网络(VN)、移动互联网以及无线通信网络分析处理感知层所收集到的数据，实现车联网网络接入、数据分析、数据传输以及车辆节点管理等功能[33]。网络层还为终端用户提供实时的信息交互以及无线资源的分配，达到信息负载的平衡以及异构网络的无缝衔接访问功能[20]。

网络层支持车辆与车辆(V2V)、车辆与行人(V2P)、车辆与路边基础设施(V2I)、车辆与基站(V2B)、车辆与数据中心(V2C)等车辆到车联网内任意可达实体间(V2X)的通信，除此之外还包含路边单元与路边单元(R2R)、路边单元与行人(R2P)、路边单元与基础设施(R2I)等通信。目前而言，车联网的网络层有两种标准[34]，一种是发展成熟的专用短程通信(Dedicated Short Range Communication, DSRC)技术[35]，由美国和日本提出和执行，以 802.11p 为通信协议生成网络。另一种是通过蜂窝网络实现的车辆到一切(C-V2X)，这一标准最多是由中国和欧洲提出的，利用成熟和广泛分布的蜂窝网络来满足车辆环境的低延迟和高可靠性[36]。从技术角度上看，C-V2X 的通信可靠性和稳定性均优于 DSRC 系统；但从商业应用上看，目前 DSRC 的产业链相对更成熟。在实际应用中，网络层并不单单由某一种通信方式实现，将众多通信方式结合起来使用才是网络层最真实的写照，除了 DSRC 与传统蜂窝网络外，有线网络、广域网和 5G 蜂窝网络等通信方式也被应用到网络层中。图 3 给出了网络层的各部分模块，同时介绍了 V2X 网络中实体间的联系。

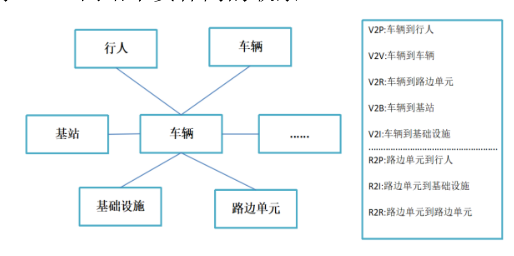


图 3　网络层模型

Fig. 3　Network layer model

chinaXiv:202205.00140v1

c) 应用层。应用层通常是软件即服务、平台即服务的缩影，应用层的设备也往往需要足够大的存储和计算能力，因此应用层经常结合云计算、边缘计算、社会计算以及普适计算等技术，从全网范围内对资源需求进行解析、计算，并合理地调配这些公共资源，实现对特定场景、任务和服务的精准认知，以达到提高驾驶员安全性与舒适性、便于交通管理的及时性与稳定性的目的。应用层面向的是用户，主要也是为用户提供不同的服务，根据用户的不同需求提供相应的软件或平台，例如实现：智慧交通、车辆管理和车载娱乐等功能。图 4 给出了应用层的各部分模块，并介绍了应用层提供的服务种类。

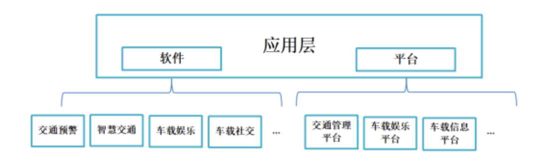


图 4　应用层模型

Fig. 4　Application layer model

1.2　车联网的性质

通过比较最新的车联网隐私保护方案，本文总结了一个成熟的车联网架构应该满足具有权衡性、适应性、可靠性和完备性四大基本性质。其中权衡性包含半匿名性[37]、半可链接性[38]、数据可用性、数据完整性和实时性。半匿名性指的就是条件匿名性，半可链接性则包含短期链接性和长期不可链接性。短期链接性是 IoV 中的一个必要属性。它的目的是为了防止一个恶意的车辆，在短期时间内恶意地发出多条信息以模拟多个车辆，导致无法抵抗女巫攻击[39]，同时，短期链接性对用户的位置隐私不产生影响，因为车辆的位置隐私不受轻微增量的影响。长期不可链接性也是 IoV 的一个必要属性，它同时也是不可追踪性的基础。攻击者将无法通过将单一车辆接收到的信息链接到车辆位置、车型和应用程序等属性来识别车辆[40]。

适应性包含灵活性、低开销和低存储。灵活性是为了满足车辆移动性的特点，低开销低存储是为了适应车辆计算、存储资源有限的特点。

可靠性包含抵抗攻击性，能够抵抗各种攻击，例如能够抵抗拒绝服务攻击(DoS)[41]、中间人攻击(MITM)[42]、推理攻击[43, 44]等，在本文的第 2 章中将会总结一些现有的车联网隐私攻击方法。此外可靠性还包含全向安全性[45]和黑盒性[46]，其中全向安全性即为前向安全性和后向安全性。

完备性包含设施完备[47]、连通性[48]、身份验证[49]和信誉机制[50]。设施完备与连通性将会在第 2 章车联网的系统架构中详细介绍。上述内容已经总结了一个成熟的车联网应该具有哪些性质，其中包括权衡性、适应性、可靠性和完备性，图 5 是对这四个性质的归纳，本文基于这四个性质展开调查，研究了近些年车联网的发展历程。

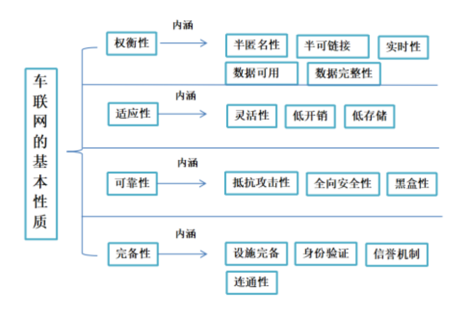


图 5　车联网的基本性质

Fig. 5　Basic properties of iov

1.3　现有的车联网隐私攻击

车联网中的攻击者可以分为 4 种基本类型：外部攻击者与内部攻击者、被动攻击者与主动攻击者、恶意攻击者与理性攻击者、局部攻击者与全局攻击者[51]。外部攻击者是指未在 TA 处注册且不属于车联网中的攻击者，内部攻击者是在 TA 中注册的合法车联网用户，可以利用所拥有的有效证书和合法身份进行恶意操作；被动攻击者可以发动窃听、监听等攻击，主动攻击者可以发动窜改、重放等攻击；恶意攻击者仅为了破坏网络稳定性、攻击用户而发起攻击，并非出于个人利益，理性攻击者对网络发起攻击的目的是为了自身获利，通常不会大肆破坏而是盗取或窜改数据；局部攻击者只能在有限范围内发起攻击，全局攻击者可以在全网范围内发起攻击。本节基于车联网的三层结构将车联网中常见的攻击按照感知层、网络层和应用层分成 3 类进行归纳总结。感知层的攻击方式包含侧信息攻击[52]、欺骗攻击[53]、节点捕获攻击[54]、窃听攻击[55]、干扰攻击[56]和窜改攻击[57]。网络层的攻击方式包含中间人攻击(MITM)[58]、重放攻击[59]、模拟攻击[60]、女巫攻击[39]和关联性攻击[61]。应用层的攻击方式包含拒绝服务攻击(DoS)[62]、恶意服务商攻击[63]、口令猜测攻击[64]、推理攻击[65]、链接攻击[66]、机器学习攻击[67]和量子攻击[68]，图 6 对这些攻击方式进行了简单的介绍。

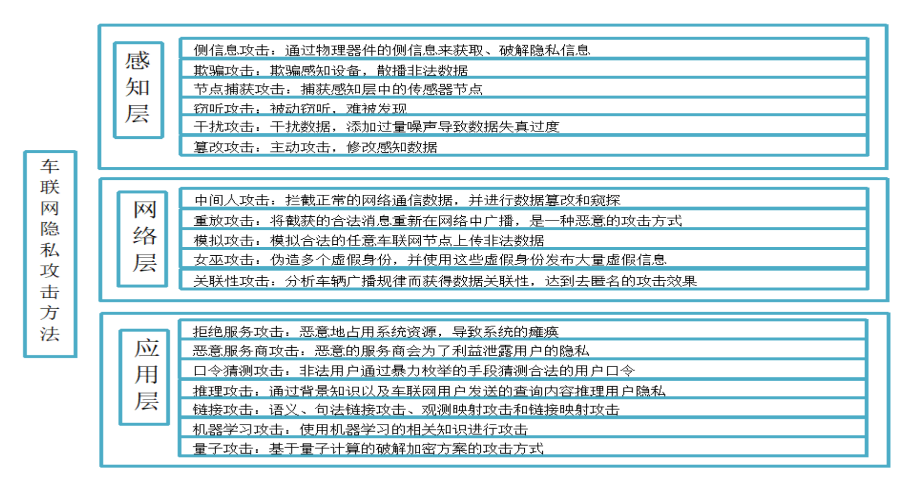


图 6　车联网隐私攻击方法

Fig. 6　Privacy attack methods of IoV

2　基于车联网架构的隐私保护

车联网中的隐私保护问题始终是用户关注的焦点，已经有大量研究人员在车联网的隐私保护方面做了长足的研究，在本章中将会回顾部分近些年车联网隐私保护的研究。基于车联网的三层架构，本章也将这些隐私保护方法分为三层。

chinaXiv:202205.00140v1

ChinaXiv合作期刊

2.1 基于感知层的隐私保护

感知层中充斥着大量的传感设备，这些传感设备就对应着客户端，是数据的产生者，也是要保护的对象。在感知层中，被攻击的是物理设备，因而在采取保护手段时也有较大的限制，目前主要有两类保护方式：基于模糊的隐私保护和基于密码学的加密方式，如图 7 所示。

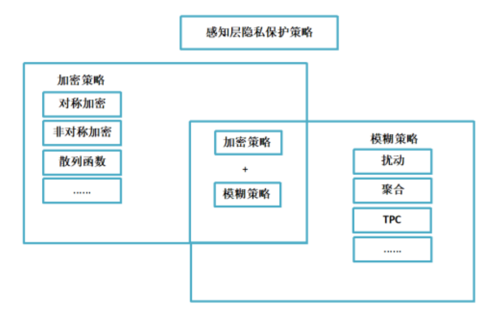


图 7　感知层隐私保护策略

Fig. 7　Privacy protection strategy of perception layer

基于模糊的隐私保护方式通常是在原有数据的基础上添加噪声或对数据进行泛化，是建立在一定的数据失真基础上的保护方式。而传统密码学的加密手段，则是在数据传输之前进行加密处理，由于加密算法的限制，基于加密的保护方式往往开销较大。差分隐私是一种基于模糊的隐私保护方法，差分隐私的定义在定义 1 中给出。

定义 1　差分隐私 [69]。给定一个随机化的算法 M，P_M 为 M 的所有可能的输出集合，如果算法 M 在任意邻居数据集 D 和 D'上的输出结果 O(O∈P_M)满足公式(1)，则 M 满足 ε -差分隐私，隐私预算参数 ε 表示隐私保护程度， ε 越小，隐私保护程度越高。

$$\Pr[M(D)\in O]\le \Pr[M(D)\in O]\times e^{\varepsilon} \tag{1}$$

差分隐私的主要思想是通过添加噪声而不改变数据本身的统计学意义，借此来保护隐私数据，常用的噪声机制有拉普拉斯机制[69]、指数机制[70]和高斯机制[71]等。差分隐私是一种定义极为严格的隐私保护模型，因能够防止攻击者拥有任意背景知识下的攻击并提供有力的隐私保护，受到了极大关注并被广泛研究。早期的差分隐私[72, 73]研究主要是基于一个可信的管理者，而在感知层中能够依靠的只有本地设备，因此局部差分隐私(LDP)是感知层中常用的隐私保护方法，局部差分隐私也叫本地化差分隐私，与早先基于可信管理者的差分隐私不同，局部差分隐私添加噪声的过程不依赖其他设备，而在本地进行[74]。现有的局部差分隐私保护技术是基于一个独立的系统结构，它是一个仅由客户端(即移动设备)和服务器组成的 C/S 结构。用户根据需要独立执行扰动机制，直接扰动受保护的数据，发送给服务提供商，获得相应的查询结果。由于没有第三方安全瓶颈的限制，系统结构简单易实现，但客户端只对自身进行干扰处理，如果完全忽略发布位置和实际位置的真实环境信息导致较大的偏差，不仅位置容易被攻击者过滤，而且降低了用户获得的服务质量；如果发布位置接近实际位置，则很容易公开用户的位置语义。因此，IoV 的局部差分隐私保护方案需要与真实的环境信息相结合，平衡隐私保护的有效性和可用性，以便进一步研究[75]。

在 2015 年，文献[76]考虑了释放的扰动位置对即将到来的释放位置的时间影响，描述了扰动位置与马尔可夫链的时间相关性，并根据位置转移先验概率构建了随机响应候选位置集。但该算法的计算复杂度相对较高，且当用户的响应位置集出现在较高概率的可能位置时，很容易暴露用户的兴趣点。在 2016 年的文献[77]中提出了一种个性化计数估计协议(PCEP)，在基于用户偏好约束的情况下，未考虑真实道路网络环境下的随机响应候选位置集。在 PCEP 算法中，所使用的 S-Hist 扰动算法的计算代价与用户数量呈正相关。当用户长时间忙碌时，计算成本巨大，采样过程也会带来一定的精度损失，需要提高算法的可用性。在 2019 年文献[78]中采用 Voronoi 图划分方法，使 Voronoi 网格至少包含一个道路节点，且没有将不可到达的区域(如河流、湖泊等)划分在安全区域中。但实际上，本文可以直接选择 Voronoi 网格边界内的其他用户的真实位置作为候选位置集，而不考虑 Voronoi 网格的位置可访问性。在 2020 年，文献[75]基于局部差分隐私和博弈模型，设计了一种隐私保护的车辆位置获取算法，该算法首先对道路网络空间进行网格划分。然后，将动态博弈模型引入到博弈用户位置隐私保护模型和攻击者位置语义推理模型中，从而在最大限度地提高服务可用性的同时，最小化暴露 k 位置集的区域语义隐私的可能性。

还有学者曾提出通过传输功率控制(transmission power control, TPC)的方式来保护隐私[79]，但在 2019 年，文献[80]通过实验分析得出窃听者数量、无线信道损伤和硬件限制与 TPC 的有效性有关，最后推翻了 TPC 作为隐私保护方案的可能性。除此之外感知层中还有很多基于密码学的隐私保护方法。2015 年，文献[81]提出了一个基于云的 RFID 认证方案。它有效地隐藏了标签的身份信息，而在不同的会话中忽略了必要的更新，容易遭受后向安全性攻击。与文献[81]所提方案类似，文献[82]在 2017 年提出了一种基于云计算的更安全的解决方案。为了满足更高的安全性要求，每次会话都在标签中进行多次哈希操作，对标签的计算性能构成了严重的挑战，从而带来较高的成本。2019 年，文献[83]提出了一种基于排列矩阵加密的轻量级 RFID 认证方案，该方案能够抵御一些典型的攻击，保证用户的个人隐私和位置隐私，但该算法的标签长度过长，加密算法可以进一步优化。2020 年，文献[84]提出了一个基于区块链的组密钥协议，基于双线性 Diffie-Hellman(DBDH)问题的复杂性保证了车联网组内节点认证的安全性。

2.2 基于网络层的隐私保护

网络层是车联网中最复杂、最开放、最易受攻击的部分，在网络层中不仅需要保护用户的数据隐私和位置隐私，还需要保护用户的身份隐私和身份验证的安全性。在该层中主要使用的隐私保护方法可以分为三类：基于匿名的隐私保护、基于模糊的隐私保护和基于密码学的隐私保护，如图 8 所示。

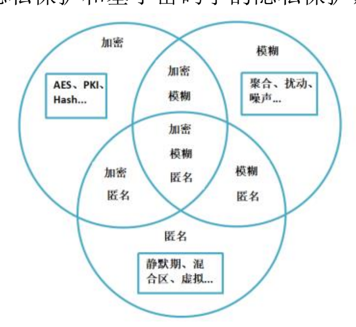


图 8　网络层隐私保护策略

Fig. 8　Privacy protection strategy of network layer

基于匿名的方法需要满足三类匿名性约束：k-匿名性[85]、l-多样性[86]或 t-最近邻[87]。k-匿名是最早提出的匿名性标准，同时也是使用最为广泛的，k-匿名是指当任意一条数据 D 在任意时刻 t_i 采样时，至少有 k-1 条数据在相应的采样位置上与 D 泛化为同一区域，则数据 D 满足 k-匿名。k-匿名技术的核心思想是将敏感属性泛化，使得单条记录无法和其他 k-1 条记录区分开，进而实现数据的隐私保护。

在车联网中通常使用的匿名策略有：组签名、混合区、静默期、虚拟机制等。组签名和混合区通常采用一种分组的形式，在组中的成员都是使用假名进行通信，且组中的成员

chinaXiv:202205.00140v1

ChinaXiv合作期刊

chinaXiv:202205.00140v1

数量越多，对应 k-匿名性中的 k 值就越大，隐私保护程度就越强，因此在应用中可以通过调节分组成员的数量来实现个性化的隐私需求，在该方案中需要考虑假名和分组的更换机制以及身份的认证机制等。静默期机制是指车辆通过采用间断式连接车联网的方式来阻断攻击者的链接攻击。虚拟机制是基于道路车辆的不确定性因素而提出的，并不是每条街道无时无刻都有足够满足 k 值的车辆进入假名分组中，因此该方法通过制造虚拟车辆的方式来保证 k-匿名性。

车联网中基于模糊的隐私保护方法除了上一节中提到的差分隐私之外，还有地理不可分、空间遮蔽等泛化方式。与差分隐私的方法类似，地理不可分和空间遮蔽的方法也是基于一定的数据失真，采用先泛化再上传的机制来保护隐私。在网络层中基于密码学的加密的方式与感知层中的加密方式有所不同，主要的区别在于网络层中的设备更广泛，因此加密的计算开销也可以通过结合边缘计算、云计算等方式来解决，通过融合这些计算范式，基于加密的保护方法也有了更好的应用前景。

在基于匿名策略的研究中，文献[88]在 2018 年提出了一种称为动态移动组定位服务(MoGLS)的车联网定位服务机制，该机制利用聚集的间接位置更新来提供满意的服务可靠性，同时降低了开销，但是方案忽略了位置的语义信息，可能造成用户的兴趣点被泄露。在 2019 年文献[89]提出了一种基于动态假名交换区的车辆位置隐私保护方案。为了避免频繁的笔名交换带来的高通信和计算开销，引入了笔名更新和笔名交换相结合的方法。在车辆密集的区域，采用了一种自适应的包围方法来降低通信开销，但在车辆不密集的场景下方案可行性较低。在 2021 年，文献[90]基于虚拟位置提出了一种车联的位置隐私保护方法，根据匿名熵和有效距离，提出了一种道路限制条件下的虚拟位置选择算法，但文章只能解决快照查询下的位置隐私问题。

在基于模糊的隐私保护方案中，文献[91]在 2018 年提出了一个基于聚合的车联网保险隐私保护方案。在 2019 年，文献[92]采用基于差异隐私的方法来保护电动汽车车主的位置隐私，并设计一种有效的电动汽车竞价与充电的在线拍卖方案，该方案能够将有限的能源分配给具有多单元用电需求的电动汽车，并与电动汽车和地理分布充电站相匹配。在 2020 年，文献[93]用一组兴趣点(POIs)代替 GPS 信息来模糊位置信息从而提出了一种保护隐私的在线出租车系统，但该方案基于基本的非交互式密钥交换协议，不能抵抗中间人攻击。文献[94]在 2021 年提出一种隐私保护的移动众包方案，结合了位置混淆和路径优化，从而以最小的成本增强了隐私保护，应用地理不可分辨性和指数机制来实现增强的隐私保证。

对于基于加密的保护方案，2019 年文献[95]设计了一种新的基于区块链的可搜索公钥加密方案用于云辅助的车联网社交网络，同时保证了前向安全性和后向安全性，但计算的复杂度较高。在 2020 年，文献[96]提出了一个基于博弈论和数据加密的个性化隐私保护框架。首先设计了一种个性化的隐私测量算法来计算用户的隐私水平，然后结合博弈论来构建一个合理的上传策略。此外，文章还提出了一种隐私保护的数据聚合方案，以确保数据的保密性、完整性和实时性。在 2021 年文献[97]提出了一种新的数据加密方法，称为动态数据加密策略(D2ES)。该方法旨在选择性地加密数据，并在时间约束下使用隐私分类方法，通过在所需的执行时间要求内使用选择性加密策略来最大化隐私保护范围，该方案可用于基于云的车联网体系中的车辆大数据上传前的加密处理。

2.3 基于应用层的隐私保护

应用层由于已经得到了经过感知层和网络层处理后的数据，这些数据可能已经是带噪声、加密或者是聚合、模糊化的数据，因此在网络层中需要解决的隐私问题主要来自于恶意的服务提供商，一个恶意的服务提供商可能会对隐私保护下的车联网数据进行推理分析，进而侵害用户的隐私。除此之外服务提供商本身的可抗攻击程度也与用户隐私息息相关。在 2021 年 6 月，一批据称从暴露 Azure BLOB 容器中窃取的奥迪与大众客户数据正在黑客论坛上公开出售[98]。由此可见服务提供商本身的单点问题是应用层隐私保护的重点。缓存、区块链、边缘化等技术被应用于解决服务提供商的单点问题。

基于缓存技术的方案其实是通过减少与服务提供商的数据通信频率来实现隐私保护，在 2019 年，文献[99]利用假名身份验证来提供隐私增强的消息身份验证和完整性，以便与其他用户、对等方以及基础设施实体进行通信，还利用一小部分为其他人服务的用户(称为服务节点)共享缓存的兴趣点数据。当用户从信息共享系统中受益时，该方案最小化了用户对 LBS 服务器的暴露。在 2020 年，文献[100]结合 l-多样性和高速缓存技术来保护位置隐私和查询隐私并减少第三方的参与，通过移动 P2P 环境中用户之间的协作来保护用户的隐私。在 2021 年，文献[101]将公交车作为文献[100]中的服务节点，提出一种基于公交车缓存的车联网位置隐私保护方案。由于公交车移动具有规律性且便于管理，该方案在城市道路中可以达到更好的效果，但在面临堵车、车辆稀疏等情况时受到较大限制。

对于区块链和边缘化的方案，实际上都是基于分布式存储或计算的原理来实现去中心化的隐私要求。文献[102]提出了 V2X 协同缓存与资源分配机制，实现车联网内计算、缓存和通信资源的有效分配；利用图着色模型为卸载用户分配信道；采用拉格朗日乘子法对功率与计算资源进行分配。不仅解决了传统的基于云的车联网结构的单点问题，还提高了整体系统的效率和资源利用率。区块链[103, 104]是一个存储时间排序数据的分布式数据库。所有参与者共同努力，在一个分散的网络中维护分布式数据库。具体来说，区块链支持受信任和保护隐私的数据存储，而不信任任何组织。此外，区块链还配备了一种激励机制，可以用来激励用户维护区块链，基于这些原因可见区块链非常适合应用于车联网的隐私保护。在 2019 年，文献[105]基于区块链技术提出了一个车联网数据共享系统，该系统实现了车联网的去中心化，但系统的吞吐量是一个问题。文献[106]提出了基于双层链的 IOV 隐私保护系统。对实时道路隐私数据进行加密，确保数据的隐私性和完整性；利用半中心化的车联网双层链结构，有利于政府或权威机构的监管，同时减少系统渠道资源的支出。同时，在零知识证明的基础上，提出了 RSA 数字签名协议。它防止路边单位从签名中获取任何信息，并自动为双层链车辆网络建立私有数据保护系统。此外，它还提高了传统模型中的数据可信度，减少了车辆网络中过度的信道资源消耗，禁止对手伪造 RSU 获取信息。在 2021 年，文献[107]提出了一种新的无云服务器的车联网的分散化体系结构。这项工作还提出了一种使用区块链机制保护事件信息和车辆身份验证的协议。在此协议中，注册用户通过星际文件系统(IPFS)[108]安全地访问事件信息。通过将 IPFS 和区块链结合，以完全分布式的方式存储信息。

3 现有研究与挑战

上一章已经基于三层架构介绍了车联网中隐私保护的研究现状，在本章中将进一步介绍更多的车联网隐私保护方案，并通过对比进行研究。由于车联网中的隐私分为数据隐私、身份隐私和位置隐私三类，本章基于这三类隐私展开研究。根据本文总结概括出的车联网的四项基本性质，本文基于这四项性质对不同的方案，依照强、较强、较弱、弱四个等级

ChinaXiv合作期刊

进行分析。

3.1 数据隐私

本节对比了近些年的车联网数据隐私保护方案，并在表 1 中给出了方案的年份、文献、应用场景、关键技术以及对车联网四个基本性质的分析，文献[95,105-107,114,116,119-121,123]都是基于区块链技术的数据保护方案，通过对比发现，这些方案的可靠性通常只能达到较强水平，这是因为区块链的底层加密采用了椭圆曲线，这不能够抵抗量子攻击，除此之外，文献[95,107,121]的完备性也只能达到较强水平，这是因为这些方案缺少了信誉机制。在权衡性方面，基于区块链技术的评级之所以只能达到较强水平是由于忽略了实时性，或者是没有提供半匿名性。基于区块链技术的方案在适应性方面的评级介于较强和较弱之间，这是因为不能满足灵活性和低开销。

表 1　数据隐私保护方案分析

Tab. 1　Analysis of data privacy protection scheme

年份	文献	应用场景	关键技术	权衡性	适应性	可靠性	完备性
2018	动态可伸缩的椭圆曲线加密策略[109]	车载安全	椭圆曲线、密码学	较强	较强	较强	较弱
	实时流量数据分析的 IoV 分布式架构[110]	车联网	云计算、雾计算	较强	强	较弱	较弱
2019	基于区块链的可搜索公钥加密[95]	云辅助车辆社交	区块链、可搜索公钥加密	较弱	较弱	较强	较强
	基于区块链的车联网安全数据共享系统[105]	车联网数据共享	区块链、盲签名、阈值机制	较强	较强	较强	强
	基于双层链的 IOV 隐私保护系统[106]	车联网	双层链、零知识、数字签名	较强	较强	较强	强
	基于本地信息感知的 IoV 信息传播方案[111]	ITS 车联网	概率转发	较弱	较强	较弱	较强
	基于深度学习的车联网隐私增强数据采集[112]	车联网	机器学习、边缘计算	较弱	较弱	较强	较强
2020	隐私保护的车联网计算资源协同调度策略[113]	边缘计算 IoV	卡尔曼滤波器、双 DQN	较弱	较强	较强	较弱
	基于区块链的车联网自适应信任管理[114]	车联网	智能合约、区块链	较强	较强	较强	强
	基于雾的 IoV 用户计算卸载[115]	雾辅助的 IoV	雾计算、博弈	弱	较强	较弱	弱
	基于区块链的 IoV 信任管理[116]	车联网	区块链、共识机制、组签名	较强	较强	较强	强
2021	基于区块链和 IPFS 的车联网认证存储[107]	无云车联网	区块链、IPFS	较强	较强	较强	较强
	基于湿度计算的智能城市车联网体系结构[117]	智慧城市	MC(Moisture Computing)	弱	强	弱	较强
	基于云的 VANET 安全路况监测[118]	云辅助车联网	第三方	较弱	强	较强	较强
	基于区块链的车辆边缘计算网络(IoVEC)[119]	边缘计算 IoV	区块链、智能合约	较强	较强	较强	强
	基于区块链的 IoV 分布式信息跟踪系统[120]	车联网	区块链	较强	较强	较强	强
	基于深度强化学习和区块链的车辆众感知[121]	车辆众感知	深度强化学习、区块链	较弱	强	较强	较强
	支持 SDN 的移动边缘计算中车联网服务卸载[122]	SDN 车联网	局部敏感哈希、边缘计算	较强	强	较强	较强
	基于信誉积分的共谋攻击节点检测方法[123]	路况信息共享	区块链、聚合	较强	较强	较强	强

通过观察表可以发现，没有任何一个方案的评级能够达到全强的程度，甚至有一个强都是很难的，这是因为大部分方案都只考虑了一个很小的范畴，例如文献[107,115]，这两个方案都更加侧重于车联网的系统效率而在隐私方面的贡献则比较小，因此在权衡性上的评价很低，这并不意味着这样的研究就没有意义，因为实际上效率本身也是权衡性的半壁江山，通过完善隐私保护的策略，就可以使得权衡性得到更好的满足。

另外绝大部分基于密码学的方案都没有考虑量子攻击对于方案可靠性的影响，这也是众多方案的不足之处，文献[110,118]还可能出现第三方的单点问题。在适应性方面，基于加密[95]、群签名[105]、边缘计算[112]、聚合[123]等技术的方案灵活性较低、开销较大，因此评级只能在较强和较弱之间。基于机器学习的方案[112,121]在平衡性上的评级较低，这是因为基于机器学习的方案需要较多的时间用于训练，这给系统效率带来了很大的负担，同时训练集本身的数据可用性也对系统有一定影响。在可靠性方面，所有提到的方案的评级都没有达到强的水平，这是因为这些方案均不能满足抵抗攻击的要求，如不能抵抗量子攻击[95,105-107,109-123]、内部攻击[95,117-118]，也有一些方案[110]不满足全向安全性。在完备性方面，文献[109-110]因为缺少身份认证和信誉机制，所以评级为较弱，其中文献[109]是一个动态可扩展的椭圆曲线加密方案在车联网中的应用，方案更加注重加密策略的研究而没有适应好车联网这个应用环境，文献[110]基于车辆、雾节点、云服务三层架构提出了一个隐私保护的车联网体系，但文章没有考虑恶意雾节点问题。

3.1.1 基于区块链的车联网数据隐私保护

本文发现近些年车联网数据隐私保护常常与区块链技术结合使用，因此将上面提到的基于区块链技术的数据保护方案进行比较研究。

在 2019 年提出的方案中，文献[95]提出了一种基于区块链的可搜索公钥加密方案应用于车辆社交网络。该方案不仅利用智能合约来消除中央服务器的单点问题，而且还支持向前和向后的隐私，从而尽可能减少信息泄露。但搜索算法的时间代价随着匹配索引数量的增加显著增加，受到网络共识机制的限制较明显，在搜索量级较大时该方案的效率较低。文献[105]提出了一个基于区块链的安全数据共享系统，采用激励机制鼓励参与者积极、诚实地广播公告信息，同时保证用户的隐私。但该方案的关键贡献是结构，而不是任何潜在的性能提高。采用的区块链系统存在局限性。如果一个事务位于来自两个不同区域的两个实体之间，那么事务率就不够高。文献[106]构建了 IOV 双层链模型，模拟了方便政府监督的半中心化系统，设计了基于零知识证明(ZKP)的 RSA 协议，为系统带来安全性和零知识属性；最后，给出了该基于双层链的 IOV 隐私保护系统的应用场景，可在车辆共享行业中得到广泛应用。但双层链的通信吞吐量低于单层链模型，数据采用对称加密的方式，在密钥的管理与分配过程中可能会产生泄露，同时也无法抵抗量子攻击。

在 2020 年提出的方案中，文献[114]提出了一种基于区块链技术的分散方案，即物联网路边单元(RSU)平面的信任管理方案。处于边缘的 RSU 协作地维护更新、可靠和一致的车辆信任值，帮助以分散的方式实现本文的目标。但没有考虑错误行为检测和局部检测使用的合理性因素、过滤器、一致性(位置、速度、航向)、信标频率等。文献[116]基于身份的组签名，提出了一种新的隐私保护声明协议。设计了一种基于区块链的信任管理系统，其中 RSUs 采用加权和的方法来

chinaXiv:202205.00140v1

ChinaXiv合作期刊

评价车辆的声誉。使用了混合 PoW 和改进的 PBFT 共识机制，以提高验证的效率。但依赖 RSU 评估车辆的声誉，局限性较大，灵活性不足，随着信息数量的递增，时间开销也线性递增，在密集场景实时性差。

在 2021 年提出的方案中，文献[107]提出了一种新型的无云服务器的车载自组网(VANET)的分散化架构。该工作还提出了一种使用区块链机制保护事件信息和车辆身份验证的协议。在该协议中，注册用户从行星际文件系统(IPFS)安全地访问事件信息。文献[119]提出了联合区块链和智能合同，以在边缘计算辅助的 IoV 中完成一个分散的可信数据共享管理系统。该系统允许车辆通过产生声誉评级来验证来自邻近地区的信息的可信度。利用激励机制触发车辆诚实存储和共享数据，从系统中获得一定的奖励。但区块链的可伸缩性限制较大，身份验证机制也依赖声誉评级来完成，虽然提高了效率但隐私保护程度较低。文献[120]提出了一个管理相关信息的系统参考模型来显示区块链如何支持 GDPR 兼容的车联网解决方案，并基于意大利的 GDPR 作为参考场景。但缺乏系统的性能评估、成本分析，应用场景依赖结合意大利法律支持的通用数据保护条例，有较大的局限性。文献[121]基于区块链技术提出了一种针对 5G 车联网的安全车辆众感架构，设计了一个深度强化学习(DRL)支持的算法来选择适当的活动矿工和交易，其目标是最大化区块链的安全性和最小化区块链的延迟。提出了一种基于非正交多址访问(NOMA)的基站中的子信道分配问题，并提出了一种基于双边匹配的算法来减少最大上传延迟。但区块链吞吐量随 RSU 数量的增加而减少，且在该架构中 RSU 充当区块链中矿工的角色，实际情况中 RSU 只是一个网关，不具备充当矿工角色的能力，在车联网中适应性较差。文献[123]提出了一种基于信誉积分的路况信息共享中共谋攻击节点检测方法。在路况信息聚合过程中，设计了恶意信息检测算法，能够检测到共谋节点发布的虚假消息，保证系统中传递消息的真实准确。但恶意行为特征检测的准确率还可以提高，在恶意节点超过 2/3 时，恶意节点被检测出来的概率低于 80%，且随着恶意节点的增多，检测成功率快速下降。

通过比较这些方案可以发现，基于区块链技术的车联网数据隐私保护都有着去中心化的特点，能够较好地解决数据孤岛和隐私泄露问题，但普遍也存在效率问题[95,105]、吞吐量问题[106,121]、局限性问题[116,119-120]，除此之外，基于区块链的数据隐私保护方法通常为了提高效率而采用轻量级的加密策略[107]，显然这无法抵抗量子攻击等新兴攻击模型，在隐私保护要求不高的情况下，这样的策略是可行的，但从普遍意义而言，车联网的平台或是软件都应该有能够提供足够强隐私保护的能力，至于是否需要提供强隐私保护可以由用户根据个人需要来确定，因此在设计基于区块链的隐私保护策略时，应该尽可能地考虑强隐私与高效率的平衡性问题，并根据用户需求自适应地调节隐私级别。由于区块链中的共识机制，当恶意用户联合起来对车联网进行恶意破坏时，系统可能会达成错误的共识，这将导致整个车联网的混乱，用户共谋的问题是一个理论存在但实际生活中不容易存在的问题，因为多数用户都是利益驱使的用户，只有在共谋破坏时获得的利益要高于安分守己时获得的利益，用户才容易成为一个共谋节点，因此只需要将奖励机制与惩罚机制应用于车联网，就基本可以在根源上解决共谋问题，也就是所谓的预防共谋攻击。针对共谋攻击，预防是较容易实现的解决方式，但百密一疏，一旦真正发生共谋攻击，所有涉及车联网的应用都可能会遭受巨大的打击，这对于那些良好的用户、服务提供商乃至整个社会都是破坏性极大的，所以在使用基于区块链技术等可能遭受共谋攻击的技术时，都有必要考虑检测共谋攻击的方式，这样才能保证系统是足够安全可靠的。

3.1.2 基于转移计算的数据隐私保护

根据调查还发现，转移计算的方式也常用于保护车联网中的数据隐私。因此将表 1 中提到的基于不同计算范式的数据保护方案进行比较研究。

在 2018 年的方案中，文献[110]开发了一个 IoV+雾计算+云计算构成的道路网络交通测量大数据分析框架，用于实时收集和处理智能车辆生成的事件，以及可视化显示每个路段的交通状态。但所开发的框架没有用大量的数据进行测试。IoV 中的互操作性问题尚未得到处理，抵抗攻击的能力较差。

在 2019 年的方案中，文献[112]设计了一种基于深度学习的数据采集和预处理方案，在边缘层进行数据过滤，清除大量的相似数据和无关数据。如果边缘设备不能独立处理一些复杂数据，则将处理后的可靠数据发送到云端进行进一步处理，最大限度地保护用户隐私。但未考虑边缘节点的不可信问题或边缘节点遭受攻击的情况，将 RSU 作为边缘节点进行预处理，但车联网中的 RSU 在计算和存储能力上受到限制，因此方案在车联网中的适应性较差。

在 2020 年的方案中，文献[113]设计了一个多区域、多用户、多 MEC 服务器系统，在每个区域部署一个 MEC 服务器，并采用 DoubleDQN 算法求解最优调度策略。但只考虑与任务传输相关的无线资源和与任务计算相关的计算资源分配。未考虑实际卸载的资源，如回程网络有线通道、数据中心内存和缓存资源。文献[115]提出了启用雾的 IoV 环境中的分散多用户计算卸载，在用户之间建立了一个合作的斯塔克尔堡博弈来进行卸载任务的选择。但延迟较大，且随着任务、用户数量的递增而线性增长。

在 2021 年的方案中，文献[117]提出了一个新的称为湿度计算(MC)的计算概念，部署在远离网络的边缘，又在云基础设施之下。与边缘和云基础设施相比，MC 减少了网络延迟，并提高了响应时间。但在稀疏网络中时，方案的效率要低于边缘计算的方式。文献[118]提出了一种基于云的 VANET 安全路况监测方案，解决本文中确定的 CVCC 挑战。但没有考虑云服务器不可信的单点问题，不可链接性过强。文献[122]开发了一个基于 SDN 的框架，将 EC 与及时调整卸载策略的能力相结合，设计了一种名为 SOME 的安全服务卸载方法。但随着服务数量的增加，服务卸载时间成比例增长，服务卸载成功率不稳定。

由于车载设备的存储和计算能力有限，云计算[118]、雾计算[110,115]、边缘计算[113,118]、湿度计算[117]等转移计算方式被用于解决这一问题。有一些车联网框架只采用一种计算范式[117-118,122]，也有一些方案在不同层中采用不同的计算范式[110,112]。采用云计算的方式时需要考虑云服务提供商的单点问题以及通信开销的问题，边缘计算的方式在一定程度上可以解决云计算的单点问题，通过将服务卸载到距离车辆最近或总体最优的边缘服务节点可以最大程度地节省通信开销，这也是众多方案试图完善的方向。湿度计算作为一个新兴范式，计算设备部署在远离网络的边缘节点，但整体处于云基础设施之下，这样的计算方式其实就是通过云来管理边缘设备，将计算、存储等任务卸载到边缘，而调度分配的工作则由云基础设施提供，这样的方式既能够解决中心化的问题，还能节省通信成本，是一个较好的方案，但方案中的边缘设备之间存在着共谋的可能，整体的安全水平还有较大的提升空间。在选择边缘节点时，车联网中的设备本身也有较大的限制，文献[112]将 RSU 作为边缘节点进行数据的预处理，然而在车联网的基础设施之中，RSU 充当的是一个网关的作用，不具备较大的存储和计算能力，只能进行简单的身份认证和数据路由，因此这样的设备并不能被选为边缘计算的节点设备。除此之外，

chinaXiv:202205.00140v1

ChinaXiv合作期刊

稀疏网络[117]和服务数量较多的网段[122]中，也面临着系统效率较低的问题。

3.2　身份隐私

本节对比研究了车联网中身份隐私的保护方法，并在表 2 中给出了一些方案的年份、文献、应用场景、关键技术以及这些方案对应车联网的四个基本性质的评级，依旧按照强、较强、较弱、弱进行划分，其中文献[49,83-84,127-130,134-143,147]都是车联网中的身份认证协议，保护用户身份隐私的身份认证方案就是匿名认证协议，指的是车辆与车辆、车辆与基础设施、车辆与一切实体节点之间的认证能够在不泄露用户身份的情况下完成，身份认证机制是车联网完备性的一部分，也就说缺少身份认证机制的车联网是不完整的，这会使得车联网中的通信变得泛滥，攻击者可以肆意占用通信资源，因此如何在保证用户身份隐私的前提下完成认证一直是车联网身份隐私保护的热点，除此之外部分研究通过假名机制来保护车联网中的身份隐私[126,143,145]。

表 2　身份隐私保护方案分析

Tab. 2　Analysis of identity privacy protection scheme

年份	文献	应用场景	关键技术	权衡性	适应性	可靠性	完备性
2016	轻量级安全协议[124]	安全协议	RSU	弱	强	弱	较强
2017	双重认证和密钥协议方案[125]	V2V 认证	信誉评价	较弱	较强	较强	强
	基于隐私保护区块链的远程认证[49]	V2X 远程认证	区块链	较强	较强	较强	较强
2018	雾计算支持的车联网隐私保护假名方案[126]	假名机制	雾计算、博弈模型	较弱	较强	较强	较强
	VANET 条件隐私保护认证方案[127]	认证协议	RSU、TPD	较弱	较强	较强	较强
	基于排列矩阵加密的安全射频识别方案[83]	射频识别认证	排列矩阵加密、RFID	强	强	较强	较强
	基于区块链技术的车联网认证方案[128]	认证协议	区块链、共识算法	较强	较强	较强	较强
2019	无证书条件隐私的车辆网络认证协议[129]	认证协议	匿名、签名	较强	较强	较强	较强
	云 IoV 中高效隐私保护的 RFID 认证方案[130]	认证协议	云计算、RFID	较强	强	较强	较强
	格基环签名[131]	车联网	格、环签名	强	较强	强	较强
	基于区块链的车联网非对称组密钥协议[84]	身份验证	区块链、非对称组密钥	强	强	较强	较强
	抗攻击信任模型[132]	车联网	假名策略	较强	强	较强	强
	基于区块链的车联网隐私保护系统[133]	车联网	区块链、工作量证明	较强	较弱	较强	强
2020	雾车辆联网隐私保护身份认证方案[134]	身份认证	雾、随机森林、公交车	较强	强	较强	较强
	基于混沌映射的会话密钥协议[135]	会话密钥协议	混沌映射、雾	较强	较强	较强	较强
	混合区的道路网络位置假名变更策略[136]	认证协议	混合区	较强	较强	较强	较强
	车联网认证密钥协商协议[137]	密钥协议	聚合签名	强	强	较弱	较强
	区块链的协同车载自组网络认证协议[138]	认证协议	区块链、数字签名	较强	较强	较强	较强
	区块链技术的轻量级匿名跨区域认证[139]	跨域认证	区块链	强	强	较强	较强
	5G 网络中安全高效的车辆组认证协议[140]	组认证协议	扩展的混沌映射、中国余数定理	强	强	较强	较强
	椭圆曲线的车联网批量匿名认证方案[141]	认证协议	椭圆曲线、分布式签名	强	较强	较强	较强
2021	改进的基于 chaff 的 CMIX[142]	认证协议	自适应布谷鸟过滤器、DH	较弱	强	较强	较强
	隐私保护的虚拟假名变更和动态分组[143]	假名交换、分组	熵、概率不可分	较弱	强	较强	较强
	无认证信号加密的 VSN 安全通信机制[144]	车辆社交网络	无证书密码体制	较强	较强	较强	较强
	移动边缘计算的车辆假名管理方案[145]	假名管理	同态加密、移动边缘计算	强	强	较强	较强
	自动驾驶匿名 VANET 通信方案[146]	自动驾驶	属性基加密	较强	较强	较强	较强
2022	后量子轻量级身份认证密钥交换协议[147]	认证密钥交换	格	较弱	强	强	较强

通过与表 1 进行比较可以发现，车联网身份隐私保护的方案通常评级更高，例如文献[83-84,131-132,137,139-140,145,147]的四项评级中有两项达到强的水平，这是因为相比于对数据隐私的保护，身份数据本身通常占用的存储更低，所需要的通信开销和计算开销也更小，这就使得这些方案[82-83,136,138-139,144]在满足快速认证的实时性上更有优势，因此权衡性和灵活性得到了较好的满足。

关于完备性，大部分的方案评级只能达到较强，其实完备性是最容易满足的一个性质，但绝大多数方案没有满足完备性的原因就在于没有考虑信誉机制，缺少信誉机制，即使方案满足可追溯和半匿名性，授权机构也无法判定什么样的用户才能称为恶意用户，也无法真正管控整个车联网的安全。

对于可靠性，仅有文献[131,147]的评级达到了强，这两个方案的共同点在于都采用基于格的加密策略，而基于格的密码学被证明是可以抵抗量子攻击的，这是一项超前的研究，也是大多数研究没有考虑的问题，因此大部分研究的可靠性评级是较强。除了不能抵抗量子攻击，还有一些方案不能抵抗推理攻击[124]、共谋攻击[136]和链接攻击[142]等。文献[124,127]是基于 RSU 的身份隐私保护方案，其安全性完全基于 RSU 的可靠性，然而实际生活场景中，RSU 是开放的基础设施，并不会因为写着“高压危险”、“有电危险”就避免被恶意用户的利用，因此两个方案的可靠性评级较低，同时灵活性也受到 RSU 的限制，因为在车辆密度较小的区域(例如：乡村)，在那样基础设施不够完善的地区可能并没有配备 RSU。

对于适应性，文献[49,125-129,131,135-136,138,141,144,146]的评级都是较强，其中文献[128,137,143,145]是由于计算或通信的开销较大，文献[125-126]是因为系统的兼容性还有待提升，其余文献都是因为方案的灵活性受限，因为车联网中的车辆高速移动对于匿名身份验证有一定的实时性要求。

对于权衡性，文献[131,142,147]没有提供条件隐私，同时也没有满足实时性的要求，因此评级为较弱，文献[143]因为匿名性和不可链接性过强，没有满足条件隐私和半可链接性，因此评级也是较弱。除此之外的大部分文献[49,128-130,132-136,138,144,146]在权衡性上的评级均为较强，之所以未能达到强的水平是因为这些方案在实时性方面有所欠缺，其中基于区块链技术的方案实时性普遍无法保证，但文献[84]同样使用了区块链的技术，不同点在于该方案还引入了轻量级的

chinaXiv:202205.00140v1

ChinaXiv合作期刊

非对称组密钥，这极大的降低了认证的时间消耗，因此较好地满足了实时性的要求。文献[124]的权衡性评价为弱，这是由于该方案完全依赖 RSU 来提供安全性，虽然文章在一定程度上保证了身份验证的安全性，但由于没有考虑 RSU 被恶意破坏的情况，这可能会造成密钥信息的泄露，因此该方案没有充分考虑权衡性。

常用的身份隐私保护方法有基于匿名和基于加密的方式，因此本文根据这两种保护方式对身份隐私的隐私保护方案进行比较研究。

3.2.1 基于匿名的车联网身份隐私保护

在 2018 年的方案中，文献[126]提出了一个三层的架构和特殊的假名雾来管理假名。提出了隐私保护的分散假名管理通信协议。但不适用于车辆稀疏的情况。

在 2019 年的方案中，文献[129]提出了一个无证书的 CPPA(CL-CPPA)协议，用于车辆环境，支持 IoV 系统中的隐私和安全要求，其中车辆和可信权限(TA)不需要分别存储任何证书用于验证和跟踪。但缺少激励机制，没有提供半链接性，没有考虑参与者不诚实的问题。文献[130]提出了一种基于云的相互认证协议，实现了标签的匿名性，不仅保护了所有者的隐私数据，还防止了外部攻击者的恶意跟踪。但基于云的方式给系统带来了较多的通信开销，也容易产生单点问题。

在 2020 年的方案中，文献[132]提出了一种轻量级信任模型，提出了在 MiTM 攻击场景中识别不诚实节点并撤销其凭证的模型。但 RSU 被认为是网络中的可信源，没有考虑 RSU 被攻击的情况以及 RSU 本身计算和存储能力的限制。文献[134]提出了基于安全认证层车辆身份认证和安全监控层的双向认证方案，以实现 IoV 的实时安全。但在车速较低或较高情况时，监控精度降低，容易出现恶意车辆被容忍的情况。分雾的划分受车流量的明显影响。文献[136]提出了一种增强型的路网用户认证密钥建立技术。给出了一种新的技术来管理车速，它可以缩短由于网络缺口问题而发生的车辆通信延迟。提出了一种新的道路网络设施的车辆隐私保护机制。但依赖 RSU 判断信息的可靠性，在部分未被 RSU 覆盖的路网中受到明显限制，随着提出请求的车辆用户数量增加，消息长度、计算时间线性递增。

在 2021 年的方案中，文献[143]提出了一种动态分组和虚拟假名(DGVP)改变方案，道路上下文信息被用来形成车辆的动态分组，在传输范围内车辆数量较少的情况下，使用虚拟假名更改策略。但由于虚拟假名在不同分组中可能会出现链接性，因此这些虚拟假名容易被恶意跟踪者通过推理攻击的方式排除，从而达到去匿名化的效果。

通过对近些年研究的调查可以看出，在基于匿名的车联网身份隐私保护方案中，混合区、虚拟、聚合等策略是较为常见的。大部分的方案都存在一个共性的问题，就是在车辆稀疏情况或者车辆较多的情况下方案效率骤降甚至出现不可用的情况[126,134,136]，这是因为这些方案主要依赖相同传输范围内的车辆来构造混合区，以此来满足匿名性，当传输范围内的车辆较少或较多时对于匿名区的构建都有一定影响，基于这样的问题，基于虚拟的方案[143]就被提出来用于解决传输范围内车辆不足的问题，通过构造一些虚假的车辆假名信息，即使传输范围内的车辆没有达到匿名性需求的 k 值时也可以用虚拟的车辆假名信息来补充匿名集以满足 k 匿名性。但基于虚拟的策略中由于虚拟假名可能存在分组之间的链接性，容易被跟踪者推理排除，导致匿名性的降低，因此在使用基于虚拟的策略是要更多的考虑虚拟假名的生成策略，使其尽可能与真实假名不可区分。基于聚合的方式通常选取 RSU[136]或云[129]作为聚合节点，在聚合节点将 k 条车辆信息进行聚合，然后将这 k 条记录的身份信息设置为一个统一标识符，以此来满足 k-匿名性，最后将满足 k-匿名性的匿名集上传给服务提供商。采用云的方式来实现标签的匿名性，与基于边缘计算方式的聚合策略相比，这种方式容易出现云服务器的单点问题，且通信开销更大。通过调查本文还发现，RSU 在一些车联网身份隐私保护方案[132,136]中充当了关键角色或者被认为是可信实体，然而 RSU 在实际生活中的车联网中充当的是一个网关的作用，该设备不具备足够的计算能力与存储能力，如果采用那些过于依托 RSU 的策略就意味着需要在全路网范围内重新布置新一代的 RSU，这样的方案存在可研究的价值，但是在实施之前也需要更多地考虑设备成本问题以及方案本身是否足够灵活。除此之外，不同的车速对于身份的正确识别也有一定的影响，在动态分组的匿名方式中由于车速变化较大或不同车辆的速度差异较大，可能导致一些车辆频繁地进入或退出某个动态分组，这在一定程度上会降低身份认证的效率，因此如何高效认证车速差异较大的车辆是一个亟待研究的问题。

3.2.2 基于加密的车联网身份隐私保护

除了基于匿名的策略，加密策略也是主要保护手段，因此本文比较研究了一些基于加密的车联网身份隐私保护方案。

在 2016 年方案中，文献[124]确保了由车辆、RSU、RSU 协调器和可信权限组成的层次结构中的节点之间的安全和高效的通信。该文提出的方法可用于减少通信过程中信息安全传输的开销。但存在节点损坏的问题。如果一个节点被破坏，那么子节点的密钥信息也被泄露。此外，父节点的关键信息也存在风险。

在 2017 年的方案中，文献[125]提出了一种新的认证方案(PPDAS)，利用双线性配对的优势来计算加密密钥，而不需要额外的密钥管理。车辆可以在不知道彼此真实身份的情况下建立会话密钥，利用身份认证和行为认证来提高决策的准确性。但随着汽车数量的增加，认证时间线性递增，在不同车速环境下，都存在一些延迟，系统兼容性较差，粒度较大。

在 2018 年的方案中，文献[49]提出了一种基于隐私保护区块链的远程认证安全模型。具有分散性、可追溯性、匿名性、不可替代性、高效性等安全特点。但随着汽车数量的增加，认证时间线性递增，使用属性基加密的方式，无法抵抗量子攻击。文献[127]提出了一种新的条件隐私保护认证协议，将批量验证作为一种验证方法，其中网络的主密钥和网络的重要信息存储在 RSU 的 TPD 中。但过于依赖 RSU 和 RSU 上的防窜改装置，需要大量更新 RSU 设备，成本较高。

在 2019 年的方案中，文献[83]提出了一种基于排列矩阵加密的轻量级 RFID 认证方案，该方案能够抵御一些典型的攻击，保证用户的个人隐私和位置隐私。该方案的认证速度快，标签的成本低，符合汽车互联网上的高速认证要求。但用于加密的替换矩阵和标签以及后台服务器共享的密钥都是固定的，这增加了信息泄露的可能性和危害性。文献[128]采用区块链框架设计新的密钥分配机制，采用区块链账本技术设计新的节点连接机制，进一步开发区块链共识技术设计新的车辆身份认证机制。但认证的效率随着区块链长度的增加而线性递增，在车辆登记和密钥分发过程中仍存在较大的包丢失情况。文献[131]提出了一种基于格困难问题的环签名方案实现了无条件的匿名性，在必要的时候还可以为授权方提供可追踪性，可以确保其在量子算法攻击下的安全性。但方案中签名内容的长度大约是环成员数量的两倍，并且与环成员数量成正比。

在 2020 年的方案中，文献[135]提出了一种基于混沌映射的全会话密钥协议方案。该方案基于切比雪夫混沌映射算法，利用混沌映射提供单向哈希；还采用切比雪夫多项式建立公共多方密钥；避免了椭圆曲线上的模乘法指数或标量乘

chinaXiv:202205.00140v1

ChinaXiv合作期刊

法。但通信成本较大，不能抵抗量子攻击，未提供全向安全性。

在 2021 年的方案中，文献[140]提出了一种安全、高效的车辆组轻量级认证协议。该方案基于扩展的混沌映射实现身份验证，中国剩余定理分配组密钥。但随着汽车数量的增加，通信和计算开销都线性递增，不能够抵抗量子攻击。文献[145]提出一种面向移动边缘计算车联网中的车辆假名管理方案，使其实现高效更新假名信息、边缘云层安全存储假名信息以及假名的可追踪。但计算开销随着通信假名数量的递增而线性递增，存在假名的撤销问题。

在 2022 年的方案中，文献[147]提出了一种适用于 IoV 架构的基于身份的两方认证密钥协议。所提议的协议消除了基于 PKI 的协议中所需的证书管理开销。此外该协议还能抵抗量子攻击。但随着汽车数量的递增，验证的效率逐渐降低，缺少批量验证的验证方式。

通过对比发现，早期的基于加密的策略[49,83,124-125,127]都没有考虑量子攻击，但近些年的研究[131,147]开始关注到量子攻击。由于量子计算机的兴起，量子攻击渐渐成为一种可能的攻击方式，而传统加密策略都是基于某个问题的困难程度来实现的，曾经可以使用几十年不被破解的密码，在量子计算的强大算力之下将被轻易破解。基于格的加密方式被证明可以有效抵抗量子攻击，近年来也得到了更多的关注，文献[131,147]是基于格的加密策略，因此能够抵抗量子攻击。通过调查发现，很多基于加密的方案[49,124-125,141,145,147]中车辆数量与认证时间成正比，这是由于这些方案是采用队列的结构依次对车辆进行验证，这样的验证方式显然可以改进，因此就有研究[126]提出批量验证的方式，批量验证就是利用密钥信息聚合之后的聚合密钥进行验证，如果聚合密钥验证通过，则所有原始密钥都验证通过，若聚合密钥未能验证成功，则采用不同的方案对所有密钥进行重新认证，例如可以采用二分法。RSU 的安全性也是一些方案[124,127]没有考虑周全的，一旦 RSU 出现损坏或者被恶意利用就会导致密钥信息的泄露，并且 RSU 是一个建立在公共信道上的通信设备，开放的通信环境使得其更容易遭到攻击，因此 RSU 应该是半可信实体和需要受保护的对象，而不是一个提供安全性的设备。基于加密的方案通常还有签名标签过长[131]、通信开销较大[135]、计算开销较大[145]等问题，因此研究轻量级的加密策略也是一个重要的研究方向，尤其是在安全系数要求较低的应用场景，减少计算和存储开销就显得更加重要。

3.3 位置隐私

本节对比了车联网中位置隐私的保护方法，并在表 3 中给出了一些方案的年份、文献、应用场景、关键技术以及这些方案对应车联网的四个基本性质的评级，除了车联网中的位置隐私，根据位置隐私引申出来的基于位置的查询隐私和连续位置下产生的轨迹隐私也是位置隐私应该保护的范畴。

表 3 位置隐私保护方案分析

Tab. 3 Analysis of location privacy protection scheme

年份	文献	应用场景	关键技术	权衡性	适应性	可靠性	完备性
2018	聚合位置更新的 VANET 分层位置服务[88]	车联网	动态分组、聚合	较弱	较强	较弱	较弱
	边缘辅助 IoV 的私人位置隐私[148]	边缘辅助 IoV	边缘计算、差分隐私	较弱	较强	较强	较弱
	实时公交 GPS 轨迹进行早期事件检测[149]	智慧城市	数据挖掘、公交轨迹	弱	强	较弱	较弱
	5G 车辆社交网络中的位置和轨迹隐私保护[150]	车辆社交网络	5G、匿名分组	较强	较强	较强	较强
	基于云辅助 VANETs 的安全位置共享[151]	云辅助车联网	代理重加密	较强	较强	较强	较强
2019	实时定位数据的高效隐私保护方案[152]	车联网	虚拟位置、匿名熵	较强	强	较强	较弱
	动态假名交换区的位置隐私保护方案[89]	车联网	假名交换、动态交换区	较弱	强	较强	较强
	基于使用的汽车保险中的位置隐私[91]	汽车保险	隐马尔可夫、博弈、聚合	较弱	强	较强	较强
	电动汽车联合招标收费在线拍卖方案[92]	电动汽车	差分隐私	较强	较强	较强	强
	有效的 LBS 查询与互隐私保护[153]	车联网	不经意传输、属性基加密	较强	强	较强	较强
2020	实时隐私保护数据发布[154]	车辆轨迹	差分隐私	较强	较强	较强	较弱
	局部差分隐私与博弈模型隐私保护算法[75]	车联网	博弈模型、LDP、*k*-匿名	较强	强	较强	较强
	在线叫车服务中的位置隐私保护[93]	在线的士	最小哈希算法、边缘计算	较强	强	较强	较强
	基于格的不经意传输位置服务方案[155]	车联网	不经意传输、格	较强	强	强	较强
	基于 VLPR 数据的车辆轨迹隐私保护方法[156]	车辆轨迹	车牌识别	较弱	强	较强	较强
2021	基于模糊的车辆云网络位置隐私保护方案[66]	云辅助 IoV	混合、静默期、协作	较强	较强	较强	较强
	基于车辆网络中虚拟位置的位置隐私保护方法[90]	车联网	虚拟、有效距离	较强	强	较强	较强
	基于公交缓存的汽车网络位置隐私保护方案[101]	车联网	公交车、缓存、*k*-匿名	较强	强	较强	较强
	自动驾驶时代车队驾驶的位置隐私保护方案[157]	自动驾驶	动态混合区	较强	较强	较强	较强
	基于车辆可靠性评估的隐私保护智能道路定价[158]	道路收费	第三方、加密	较强	较强	较强	强
	利用生成式对抗性模仿学习生成城市车辆轨迹[159]	车辆轨迹	生成对抗网络	较弱	强	较弱	较弱
	基于车联网传输范围改变的位置隐私保护方案[160]	车联网	假名机制	较强	强	较强	较强

通过竖向观察权衡性的评级可以发现这些位置隐私保护策略都没有很好地满足权衡性，这是因为这些方案的隐私保护程度太强，没有满足半匿名性的要求，这也是因为一般而言半匿名性可以通过身份验证来满足，因此这些方案考虑的是强隐私保护，其中文献[88-89]还提供了强不可链接性，容易受到女巫攻击的影响，文献[91,148,156,159]因为计算开销较大，没有平衡好实时性的要求，因此权衡性评级为较弱。文献[149]是基于公交车历史轨迹的数据挖掘研究，没有提供足够的隐私性，完全偏重数据的效用，因此权衡性的评级为弱。

适应性方面，较多的方案[75,89-91,93,101,149,152-153,155-156,159-160]都很好地满足了适应性，文献[88,154]因为受到路边单元的限制而灵活性不足，这两个方案都是将位置数据上传至 RSU，在 RSU 处进行聚合或加密操作，然后再上传至位置服务提供商，这样的方式在车辆高速移动时有着明显的限制，因为在与路边单元进行通信时要先进行身份的验证，然后再进行数据的加密传输，这样的通信开销难以满足数据实时性的需求。另外，文献[151,157]中使用了假名机制，但并没有考虑假名的撤销，这也给车联网的灵活性带来了影响。

对于可靠性方面，文献[155]的评级为强，因为该方案是基于格的加密策略，能够抵抗量子攻击，同时该方案提供的

chinaXiv:202205.00140v1

ChinaXiv合作期刊

强隐私性也能够抵御其他攻击，文献[88,149,159]因为抗攻击性较弱，且不提供全向安全性，所以被划分为较弱等级，其余的方案都被划分为较强，是由于它们不能抵抗一些攻击，例如共谋攻击[75,89,148,157]、恶意节点[92,101]、欺骗攻击[150]等。

对于完备性方面，大部分方案都没有考虑信誉机制或身份验证，其中文献[88,148-150,154,159]既没有考虑身份验证也没有考虑信誉机制，因此完备性评级较弱，但并不是说这样的研究就没有意义，因为车联网的复杂性使得其可以细化成很多子问题，这些方案之所有在完备性上欠缺是因为它们解决的就是车联网中的子问题，但在考虑整体车联网架构时本文需要将诸多方面都考虑在内，才能构建一个安全、可靠的车联网生态环境。

车联网中位置隐私的保护通常基于匿名、模糊和加密的方式，因此本文根据这三类策略进行比较研究。

3.3.1 基于匿名的车联网位置隐私保护

在 2018 年的方案中，文献[88]提出了防止由于聚合位置更新而导致的服务可靠性恶化的机制，同时充分利用聚合位置更新来减少信令开销。但过于理想化，方案基于相似轨迹的车辆构成动态分组，并以组内的一个车辆作为低级服务器，实际情况下大部分车辆即使在同一条路行驶也不太可能长期保持相似的轨迹，而且作为服务器的节点车辆也可能存在不诚实行为。文献[150]设计了一个基于 5G 的车辆社交网络(VSN)框架，提出了动态群划分算法(DGD)，该算法适合于 5G 的动态特性，并满足了 VSN 的实时需求。但没有考虑基于位置的查询隐私。

在 2019 年的方案中，文献[152]基于 k-匿名性的基本思想，提出了一种利用虚拟位置和路线混淆来保护车辆位置隐私的方案。但没有考虑来自周围车辆的攻击，当路由偏差过大的时候还是使用正常的 LBS，这也是本文的限制之处。过于理想化，实际上轨迹相似的车辆并不是足够充分的。

在 2020 年的方案中，文献[155]建立了一个基于车牌识别数据的传递时间、颜色、类型和品牌的对手模型，以评估基于时间序列的所提出的(m, n)桶模型的性能，通过不同泛化等级满足不同匿名需求。但方案的场景限制较为明显，只能用于防止车牌检测对车辆位置信息或轨迹信息的泄露。在连续跟踪的检测环境下，系统效率较低。

在 2021 年的方案中，文献[90]提出了一种基于道路限制下的虚拟位置的位置隐私保护方法，引入了有效距离来表示位置分布的特征，以提高虚拟位置的有效性。但连续场景下的可用性较低。文献[101]提出了一种安全的基于广播的位置隐私保护方案，在该方案中，公交车充当边缘节点。但道路限制较为明显，在没有公交车的部分路段该方案不可用，或公交车稀疏时，处理事务的能力也有较大的限制，广播的方式容易造成网络的堵塞。文献[157]提出了一个动态混合区来保护自动驾驶车辆在车队中的位置隐私。但存在假名的撤销问题。

通过研究发现，基于匿名的方案都有一个共同的特点就是需要构造匿名集，构造的匿名集中有 k 条不可区分的记录，这样的匿名集就满足 k-匿名性，在车联网的位置隐私保护中依靠抑制和泛化的方式来构造匿名集，抑制通常是指抑制唯一标识符(例如：车牌号)的发布，泛化的手段则有很多，例如：聚合[88]、虚拟[90,150]、混合区[157]等。文献[88]中将相似轨迹的车辆构建为一个匿名集，文献[101]将公交车作为边缘节点与其周围的车辆构成匿名集，这两个方案都是基于动态分组的混合区，除了动态的还有静态混合区策略，静态混合区通常将 RSU 或其他边缘计算设备作为分组的组头。无论是何种混合区策略都存在较为明显的限制，就是受到组头位置的限制。以动态混合区为例，无论是与相似轨迹的车辆还是公共汽车去形成稳定的、满足 k-匿名性的匿名集都是较为困难的，尤其是在路况条件不稳定和复杂路段下，这种分组的效率将会大打折扣。基于虚拟的方案[90,150]不仅可以作为单独使用的匿名策略也可以作为一种补充策略，当一些复杂路段下部分方案无法及时构建出 k-匿名集时，采用虚拟策略补齐匿名集，就能够在应对不同路况环境下更具灵活性。但基于虚拟的策略需要注意的是如何构建出尽可能真实的假数据，还需要考虑周围车辆的攻击，因为在车辆稀疏时周围车辆可能轻易地推测出真实的车辆与假名的关联，文献[150]的不足之处就在于没有考虑周围车辆的恶意行为。文献[90,155]有一个共同的问题就是在连续场景下的可用性较差，连续场景在实际车联网中是十分常见的，比如：定位导航服务，连续场景对方案有更高的实时性要求，因而需要提升系统的效率，减少开销。基于匿名的方案中还普遍存在假名的撤销问题[157]，这些方案使用了证书撤销列表来存储已经被撤销的假名，由于车联网的快速拓扑将导致证书撤销列表快速增长，进而带来额外的存储、通信和计算开销，导致系统的效率降低甚至直接瘫痪。本文还发现，基于匿名的车联网位置隐私保护应该包含位置隐私、基于位置的查询隐私以及轨迹隐私，但有趣的是很少有方案同时保护这三个隐私。

3.3.2 基于模糊的车联网位置隐私保护

在 2018 年的方案中，文献[148]提出了一种边缘辅助的车联网架构，提出了一种新的差分隐私保护服务使用框架来实现该架构的安全和隐私要求。但由于车辆缓存的限制，导致在车辆快速移动的环境中处理位置和时间依赖的缓存数据的问题。

在 2019 年的方案中，文献[92]基于差分隐私提出了一个位置隐私保护的电动车在线竞拍充电系统。但在进行充电站分配时没有考虑堵车的情况，可能出现竞拍者物理距离最近，但时空距离并非最优的情况，导致系统效率降低。文献[154]提出了一种基于差分隐私的隐私保护机制用于保护车辆的实时轨迹数据发布。但计算开销较大。

在 2020 年的方案中，文献[75]提出了一种满足 k-位置集的局部差分隐私的位置数据采集方法，引入了动态博弈模型对位置集进行优化。但在低隐私预算下，由于引入噪声大，交通密度统计结果的精度较低。

在 2021 年的方案中，文献[159]提出了一种用于城市车辆轨迹生成的生成对抗性模仿学习框架。用合成的轨迹作为发布轨迹。但没有考虑到交通条件的影响或与其他车辆的交互。

通过研究发现，基于模糊的方案是用一定程度的数据失真来换取对隐私的保护，因此该方案的核心在于效用与安全的平衡性问题。文献[75]在低隐私预算下，由于引入噪声大，交通密度统计结果的精度较低，因此应该适当地重新调整隐私预算的范围，例如：将最低可容忍交通密度统计精度所对应的隐私预算设置为最低预算值，或者通过其他方式减少噪声的引入，总之应该尽可能权衡好效用与安全的关系，避免一边倒。一些基于模糊的车联网位置隐私保护方案[92,159]还没有考虑到交通条件的影响或与其他车辆的交互问题，换句话说就是，这些方案仅仅考虑了道路与车辆的空间关系，而没有将道路、车辆和周围车辆的时空关系一同考虑。除此之外，缓存[148]和计算开销[154]也是基于模糊的车联网位置隐私保护方案中经常存在的问题。

3.3.3 基于加密的车联网位置隐私保护

在 2018 年的方案中，文献[151]基于代理重加密的方案提出了一个安全的位置共享系统，允许车辆用户与用户授权的路边单位共享其驾驶轨迹信息。但云服务提供商可能出现单点故障，车辆用户通过与用户授权的 RSU 共享轨迹信息，但 RSU 的计算和存储有较大的限制。通信开销过大，实时性

chinaXiv:202205.00140v1

ChinaXiv合作期刊

较差。

在 2019 年的方案中，文献[153]利用雾计算，采用不经传输(OT)和基于密文策略属性的加密(CP-ABE)，提出了两种保护隐私的 LBS 查询方案(kNN 和 T-kNN)。但网格粒度越大时，计算开销成指数型增长。

在 2020 年的方案中，文献[93]提出了一种基于 MinHash 算法的位置隐私保护方案，该方案可以在不泄露乘客和司机隐私的情况下有效地匹配乘客和司机。但基于基本的非交互式密钥交换协议，不能抵抗中间人的攻击。文献[155]提出一个不经意传输的扩展协议并使用格基的环学习错误(ring-LWE)方案作为不经意传输的基础，用于保护用户的查询隐私、位置服务器的信息内容和车辆的位置隐私。但交换机具体是什么设备没有理论支撑，安置在什么位置也没有说明，缺乏完整性。

在 2021 年的方案中，文献[158]提出了一种可靠的具有可信度评估的道路收费系统，该系统保证了车辆位置隐私的安全，防止了恶意车辆同时发生收费违规行为。车辆路线隐私信息被加密并上传到附近的路边单位，然后再转发到交通控制中心收费。但随着车辆的递增，验证签名的时间线性递增，不能抵抗量子攻击。

基于加密的方案可以保证数据的完整性，但因为其计算开销较大，可能导致系统效率较低，因此基于加密策略的方案需要平衡的是效率与安全的关系。随着时代发展，量子攻击成为了一种安全威胁，基于加密的方式就不得不考虑这个威胁，较多的基于加密的策略都不能抵抗量子攻击[93,151,153,158]。文献[155]以基于格基的环学习错误作为不经意传输的基础还提出一个不经意传输的扩展协议，不仅保护了用户的查询隐私和位置隐私还保护了位置服务器的信息内容，基于格的原理也使得该方案能够抵抗量子攻击。代理重加密的方式是一种借助可信第三方或半可信第三方来完成的加密策略，文献[151]就是一个基于代理重加密的位置共享系统，但该方案中的车辆依赖与 RSU 共享轨迹信息，受到 RSU 存储与计算资源的限制。基于加密的策略因为其计算开销大所以存在实时性较差的问题[151]，且随着粒度的变大，计算开销也会逐渐增大[153]。也有一些轻量级的加密方式能够极大的提高效率，但对应的系统安全性也会下降。文献[93]使用非交互式密钥交换协议，虽然系统效率得到了提升，但却不能抵抗中间人的攻击，存在较多安全隐患。

3.4　车联网隐私保护的挑战

通过对数据隐私保护方案的研究发现，早期的车联网应用通常是基于云服务的应用场景，在这样的体系结构中，云服务器几乎承载了整个系统的计算和存储压力，这样能够解决车载设备计算和存储能力受限的问题，在一定程度上可以更好地适应车联网。但基于云辅助的车联网模型容易出现单点问题，也就是说一个不可信的云服务提供商可能会造成更大的隐私泄露风险，而对于那些安分守己的服务提供商而言，即使他们不去刻意地获取用户的个人信息，也可能要面对各种各样的外部攻击，因此服务提供商需要耗费大量的人力财力去防止用户的隐私泄露。与此同时，多跳路由也是中心化架构的一大弊端，造成了较大的通信开销，在许多实时性要求较高的车联网应用中很难有好的表现。显然这种中心化的方式有着极大的弊端，web3.0[161]是一个万物互联的时代，车联网也正在朝着 web3.0 的方向蓬勃发展，传统的客户/服务器模式已经无法适应如今的车联网需求，因此研究出去中心化和分布式的车联网系统架构是车联网行业的一大挑战。

在去中心化和分布式的研究中，区块链技术引起了较为广泛的关注，与传统的中心化方式不同，基于区块链或边缘计算等分布式结构的车联网应用不需要依靠服务商的可靠性，而是通过联合车联网中不可信节点共同维护一个共识的、可信的分布式账本，数据之间的传输也可以从客户/服务器的模式变为点对点的传输，既可以提升传输的速度还可以更好地利用公共资源。IPFS 是一个面向全球的、点对点的分布式版本文件系统，采用基于内容的寻址方式，不需要验证发送者的身份，而只需要验证内容的哈希，通过这样可以让系统的文件数据速度更快、更安全、更健壮、更持久。已经有一些研究将 IPFS 应用于车联网之中，但这些研究还处在理论阶段，因为不论是区块链技术还是 IPFS，它们本身任然存在着不足，例如区块链中匿名性过度的问题，通过改进和完善这些技术，落实分布式车联网架构是一个巨大的挑战。

在车联网身份隐私的保护中，匿名身份认证是主要的研究方向，在这项研究中，如何建立假名群组、如何更换假名、如何撤销假名是主要的问题。身份认证是车联网中实体之间进行数据传递的先决条件，为了避免非法用户恶意传播、盗取数据，通信实体与实体之间需要通过认证协议来搭建桥梁，现有的认证协议较少地考虑了共谋攻击的问题，也就是说绝大多数的研究都认为可信用户更多，然后通过设置门限的方式来达成共识，最终完成认证。这样的研究理论上是可行的，因为本文主观上都认为大多数用户是诚实可信的，并且可以通过增设信誉机制来鼓励用户变得更加诚实可信，但车联网存在的风险可能会导致不可挽回的隐私泄露，因此设计能够抵抗共谋攻击的身份认证协议是车联网身份隐私保护的一大挑战。

车联网中位置的隐私保护有着最广泛的应用，因为车载应用往往都是基于位置的应用，例如导航、路况预报等。在如此之多基于位置的服务中，位置隐私，基于位置的查询隐私，连续位置下的轨迹隐私，都属于该项研究应该保护的对象。通过本文的调查发现，大部分的位置隐私保护策略都仅仅关注了位置隐私、查询隐私、轨迹隐私之中的一个或两个，只有极少数的研究同时保护了三个隐私，但实际应用中三者的隐私必须都能够保障，因此设计一个多维的车联网位置隐私保护策略是一个挑战。

除此之外，自动驾驶技术在近些年的研究中引发了越来越多的关注，自动驾驶技术离不开车联网，也可以说自动驾驶就是车联网的一个应用，如何利用车联网实现安全可靠的自动驾驶是一大挑战。

4　总结与展望

在本章中，本文将对本文进行总结，并提出一些车联网隐私保护研究中的开放性问题和研究方向。

4.1　总结

车联网具有十分广泛的应用前景，与人们的出行、交通安全息息相关，是现在也是未来研究的热点，而车联网的复杂性和特殊性也给车联网的研究带来了很多难题，由于关乎交通安全和社会稳定，因此车联网的应用必须满足安全性的要求，为用户提供隐私保护。本文根据车联网的体系结构和现有的研究总结了车联网应该具备的四个基本性质，并对这四个性质进行了详细的介绍，然后按照车联网的三层结构介绍了车联网现存的攻击模型。本文还详细介绍了现有的一些车联网隐私保护方法，并做了比较研究，通过比较研究提出了对现有车联网隐私保护研究的看法和对未来的展望。

4.2　展望

4.2.1 去中心化的车联网隐私保护

通过本文的调查发现基于云的车联网是很多车联网研究的背景基础，这里的云通常被认为是完全可信或半可信的实体，这样的架构将安全性的重任完全寄托于云。去中心化是为了防止恶意的服务提供商对车联网隐私造成不可估量的侵

chinaXiv:202205.00140v1

ChinaXiv合作期刊

chinaXiv:202205.00140v1

害，除此之外，去中心化的体系也能够防止服务提供商出现单点故障。随着边缘计算、区块链、雾计算等技术的发展，车联网数据的分布式计算及存储已经成为了可能，但由于这些分布式技术本身存在的隐私和安全问题，要如何在车联网这个应用环境下结合这些计算范式以达到隐私和效用平衡的效果，这是一个能够深入研究的方向。

4.2.2 抗量子攻击的保护方法

通过本文的调查发现绝大多数现有的车联网隐私保护方案都没有考虑量子攻击，但随着量子计算机的发展研究，传统基于复杂度的加密保护方法已经无法抵御量子计算机的强大算力，曾经能保证几十年内安全的加密策略如今将面临几秒内被破解的风险，因此车联网的隐私保护也被要求能够抵抗量子攻击，这是一项面向未来的研究。

4.2.3 灵活性更高的保护方法

通过本文的调查发现现有的研究普遍存在灵活性较差的问题，过于依赖 RSU、车辆稀疏地区可用性低、高密度地区频繁交换假名、开销较大、高速移动场景不可用是主要的灵活性较差的原因，因此采用融合性更好的方案，例如先检测周围环境再匹配合适的方案，在车辆密集处(例如城市道路)采取适应的假名交换策略，在密度较为稀疏的地区(例如乡村)采取适应的隐私保护方法，在高速移动场景(例如高速公路)采取验证速度更快的方案。通过考虑不同的场景的特殊性，自适应地选择更好保护策略，为车联网提供更好的灵活性。

4.2.4 个性化隐私

本文的研究发现现有的研究通常提供的是一种一致的隐私保护，也就是对于所有车联网中的用户都采取一样的隐私标准，可显而易见的是，不同的用户、不同的位置、不同的数据、不同的时间，对于用户个人而言需要何种程度的隐私保护是不同的，例如：当用户在兴趣点时，会更加希望此时的隐私得到更好的保护，而用户在无关紧要的位置时，通常不太需要对其进行保护。因此提供一种个性化的隐私是使得车联网隐私保护更加人性化的必然要求。

4.2.5 假名的撤销

车联网中一种常见的隐私保护方式是假名机制。当车辆驶出网络或出现恶意行为时，由授权中心(TA)撤销颁发给车辆的假名证书。本文的调查发现，现有的很多研究是使用证书撤销列表(CRL)存储已被撤销但未过期的假名证书，但车联网中车辆的高移动性会使 CRL 大小迅速增长，从而带来额外的存储、通信和计算开销。因此如何设计一个合适的假名撤销机制是基于假名机制的车联网隐私保护方案的主要问题。

参考文献：

[1] Shafi M, Molisch A F, Smith P J, *et al.* 5G: A tutorial overview of standards, trials, challenges, deployment, and practice [J]. IEEE Journal on Selected Areas in Communications, 2017, 35 (6): 1201–1221.

[2] Bhatia H. 125 Million+Connected Cars Shipments by 2022; 5G Cars by 2020 [R/OL]. 2020, (2018-04-03) [2020-12-31]. https://www. counterpointresearch. com/125-million-connected-cars-shipments-2022-5g-cars-2020/.

[3] WHO. Global Status Report on Road Safety 2015; World Health Organization: Geneva, Switzerland [R] , 2015.

[4] Alam M, Ferreira J, Fonseca J. Introduction to Intelligent Transportation Systems [J]. Studies in Systems, Decision and Control, 2016, 52: 1-17.

[5] Zhong Weiyi, Yin Xiaochun, Zhang Xuyun, *et al.* Multi-dimensional qualitydriven service recommendation with privacy-preservation in mobile edge environment [J]. Computer Communications, 2020, 157: 116–123.

[6] Xu Xiaolong, Zhang Xing, Liu Xihua, *et al.* Adaptive Computation Offloading With Edge for 5G-Envisioned Internet of Connected Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22 (8): 5213-5222.

[7] Zhou Chunjie, Li Ali, Hou Aihua, *et al.* Modeling Methodology for Early Warning of Chronic Heart Failure Based on Real Medical Big Data [J]. Expert Systems with Applications, 2021, 151: 113361.

[8] Xu Xiaolong, Wu Qi, Qi Lianyong, *et al.* Trust-Aware Service Offloading for Video Surveillance in Edge Computing Enabled Internet of Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22 (3): 1787-1796.

[9] Xu Xiaolong, Li Haoyuan, Xu Weijie, *et al.* Artificial Intelligence for Edge Service Optimization in Internet of Vehicles: A Survey [J]. Tsinghua science and technology, 2020, 27 (2): 270-287.

[10] Carlier M. Projected share of new Internet-connected light-duty vehicles [R/OL]. Statista, 2021. (2019-03-01) [2021-03-31] https://www. statista. com/statistics/275849/number-of-vehicles-connected-to-the-internet/.

[11] Abdulkadhim F G, Yi Z, Tang C, *et al.* Design and development of a hybrid (SDN + SOM) approach for enhancing security in VANET [J]. Applied Nanoscience, 2021. https://doi. org/10. 1007/s13204-021-01908-2.

[12] Al-Absi M A, Al Absi A A, Sain M, *et al.* Moving Ad Hoc Networks—A Comparative Study [J]. Sustainability, 2021, 13 (11): 6187.

[13] Huang Aidi, Motani M. A geographical segment architecture for connected vehicle networks [J]. Vehicular Communications, 2019, 19 (4): 100167.

[14] Wang Jijin, Xiao Xiaoqiang, Lu Peng. Vehicle Network Node Behavior Classification based on Optimized Bayesian Classifier [C]// Proc of the 5th International Conference on Vehicle, Mechanical and Electrical Engineering. 2019.

[15] Cramer C, Fuhrmann T. Performance evaluation of chord in mobile ad hoc networks [J]. Decentralized resource sharing in mobile computing and networking, 2006: 48-53.

[16] Seshasayee B, Schwan K. Mobile service overlays [J]. Decentralized resource sharing in mobile computing and networking, 2006, 30-35.

[17] Trappeniers L. Towards user generated applications on the internet-of-things (IoT) [J]. Advances in Mobile Computing and Multimedia, 2010: 29.

[18] Dureja A, Suman. Efficient transportation: future aspects of IoV [J]. International Journal of Vehicle Information and Communication Systems, 2020, 5 (3): 290.

[19] Afzal K, Tariq R, Aadil F, *et al.* An Optimized and Efficient Routing Protocol Application for IoV [J]. Hindawi Mathematical Problems in Engineering, 2021, 2021: 9977252.

[20] Xiao Yao, Liu Huiheng, Cheng Xiaohong. Key Technologies of Internet of Vehicles and Their Development Trends and Challenges [J]. Communications Technology, 2021, 54 (01): 1-8.

[21] Li Jianxin, Cai Taotao, Deng Ke, *et al.* Community-diversified influence maximization in social networks [J]. Information Systems, 2020, 92: 101522.

[22] Caprolu M, Lombardi F, Pietro R D, *et al.* Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues [C/OL]/ Proc of IEEE International Conference on Edge Computing, 2019. http://doi. org. 2019. 10. 1109/EDGE. 2019. 00035.

[23] Wang Xiaokang, Yang L T, Song Liwen, *et al.* A tensor-based multi-attributes visual feature recognition method for industrial intelligence [J]. IEEE Transactions on Industrial Informatics, 2020, (99): 1-1.

[24] Faisal Rasheed L, Kumar V H, Pal S K. Evolution of VANETS to IoV: Applications and Challenges [J]. Technical Journal, 2021, 15 (1): 143-

ChinaXiv合作期刊

149.

[25] 龚媛嘉，孙海波. 车联网系统综述 [J]. 中国新通信, 2021, 23 (17): 51-52. (Gong Yuanjia, Sun Haibo. Overview of vehicle networking system [J]. China new communications, 2021, 23 (17): 51-52.)

[26] 王晓，要婷婷，韩双双，等. 平行车联网基于 ACP 的智能车辆网联管理与控制 [J]. 自动化学报, 2018, 44 (8): 1391-1404. (Wang Xiao, Yao Tingting, Han SHuangshuang, *et al.* Parallel Internet of Vehicles: The ACP-based Networked Management and Control for Intelligent Vehicles [J]. Acta Automatica Sinica, 2018, 44 (8): 1391-1404.)

[27] 孟源，柴舒杨，罗正华，等. 车联网网络架构分析 [J]. 成都大学学报: 自然科学版, 2012, 31 (4): 346-349. (Meng Yuan, Chai Shuyang, Luo Zhenghua, *et al.* Analysis of Internet of vehicles network architecture [J]. Journal of Chengdu University: Natural Science, 2012, 31 (4): 346-349.)

[28] 陈娜. 车联网安全防护系统的设计与分析 [J]. 电脑开发与应用, 2014, 27 (10): 4. (Chen Na. Design and analysis of safety protection system for Internet of vehicles [J]. Computer development and Application, 2014, 27 (10): 4.)

[29] 孙晓雯，赵伟，何斌，等. 基于无线网络的物流车联网应用层设计研究 [J]. 电子测量技术, 2016, 2016 (5): 5. (Sun Xiaowen, Zhao Wei, He bin, *et al.* Research on application layer design of logistics vehicle networking based on wireless network [J]. Electronic measurement technology, 2016, 2016 (5): 5.)

[30] Juan C C, Sherali Z, Juan A G I. A seven-layered model architecture for Internet of Vehicles [J]. Journal of information and telecommunication, 2017, 1 (1): 4-22.

[31] Zeng Fantian, Li Chunxiao, Zhen Anran, *et al.* Review of the key technologies and applications in internet of vehicle [C/OL]/ Proc of the 13th IEEE International Conference on Electronic Measurement & Instruments, 2017, (2017-10-20) [2017-10-21]. http://doi. org. 2017. 10. 1109/ICEMI. 2017. 8265773.

[32] Li Zongqin. Research on the Key Technologies of IoV System Structure and Perception Layer [J]. ITU Telecom World, 2019, 2019 (1): 70-71.

[33] Ji Baofeng, Zhang Xueru, Mumtaz S, *et al.* Survey on the Internet of Vehicles: Network Architectures and Applications [J]. IEEE Communications Standards Magazine, 2020, 4 (1): 34-41.

[34] Lu Zhaojun, Qu Gang, Liu Zhenglin. A survey on recent advances in vehicular network security, trust, and privacy [J]. IEEE Transactions Intelligent Transportation Systems, 2018, 20 (2): 760-776.

[35] Li Baozhu, Gordon S, Bo Hu, *et al.* Modeling and QoS analysis of the IEEE 802. 11p broadcast scheme in vehicular ad hoc networks [J]. Journal of Communications and Networks, 2017, 19 (2): 169-179.

[36] Naik G, Liu Jinshan, Jerry Park J M. Coexistence of Wireless Technologies in the 5 GHz Bands: A Survey of Existing Solutions and a Roadmap for Future Research [J]. IEEE Communications Surveys & Tutorials, 2018, 20 (3) , 1777-1798.

[37] Hussain R, Zeadally S. Autonomous Cars: Research Results, Issues, and Future Challenges [J]. IEEE Communications Surveys & Tutorials, 2018, 21 (2): 1-1.

[38] Khan S, Sharma I, Aslam M, *et al.* Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey [J]. Future Internet, 2021, 2021 (13): 96.

[39] Douceur J R. The Sybil Attack [J]. International Workshop on Peer-to-Peer Systems, 2002, 2429: 251–260.

[40] Studer A, Shi E, Bai Fan, *et al.* TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs [C]// Proc of IEEE Communications Society Conferenceon Sensor, Mesh & Ad Hoc Communications & Networks, 2009.

[41] Park K, Lee H. On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets [J]. Applications, technologies, architectures, and protocols for computer communications, 2001: 15-26.

[42] Hwang H, Jung G, Sohn K, *et al.* A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802. 1X and EAP [C/OL]/ Proc of International Conference on Information Science & Security IEEE Computer Society, 2008. http://doi. org. 2008: 164-70. 10. 1109/ICISS. 2008. 10.

[43] Ganju Karan, Wang Qi, Yang Wei, *et al.* Property Inference Attacks on Fully Connected Neural Networks using Permutation Invariant Representations [J]. Computer and Communications Security, 2018: 619-633.

[44] Yale A, Dash S, Dutta R, *et al.* Assessing privacy and quality of synthetic health data [J]. Artificial Intelligence for Data Discovery and Reuse, 2019: 8.

[45] Cui Jie, Sun Yue, Xu Yan, *et al.* Forward and backward secure searchable encryption with multi-keyword search and result verification [J]. Science China (Information Sciences) , 2021: 1-3.

[46] Rao Jinmeng, Kang Yuhao, Gao Song, *et al.* LSTM-TrajGAN: A Deep Learning Approach to Trajectory Privacy Protection [C]// Proc of the 11th International Conference on Geographic Information Science. 2020

[47] Zhao Ping, Zhang Guanglin, Wan Shaohua, *et al.* A survey of local diferential privacy for securing internet of vehicles [J]. The Journal of Supercomputing, 2019, 76 (2) .

[48] Torre G D L, Rad P, RaymondChoo K K. Driverless vehicle security: Challenges and future research opportunities [J]. Future Generation Computer Systems, 2020, 108: 1092-1111.

[49] Xu Cheng, Liu Hongzhe, Li Peifeng, *et al.* A Remote Attestation Security Model Based on Privacy-Preserving Blockchain for V2X [J]. IEEE Access, 2018, 6: 67809-67818.

[50] Shrestha R, Nam S Y, Bajracharya R, *et al.* Evolution of V2X Communication and Integration of Blockchain for Security Enhancements [J]. electronics, 2020, 2020 (9): 1338.

[51] Raya M, Hubaux J P. Securing Vehicular Ad Hoc Networks [J]. Journal of Computer Security, 2007, 15 (1): 39-68.

[52] Cao Maosen, Wang Leibao, Hu Bo, *et al.* Multi-stage Information Physics cooperative attack strategy considering cascading faults of electro-pneumatic coupling system [J]. Power automation equipment, 2019, 39 (8): 128-136.

[53] Wang Tianyi, Zhu Fengyuan, Tian Xiaohua. Method of Eavesdropping and Spoofing Attacks on Frequency Shift Backscatter Systems [J]. Journal of Signal Processing, 2021: 1-12.

[54] Wang Chenyu, Wang Ding, Tu Yi, *et al.* Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks [J]. IEEE Transactions on Dependable and Secure Computing, 2020, 2020: 1-1.

[55] Wang Chenyu, Wang Ding, Xu Guoai, *et al.* Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4. 0 [J]. Science China (Information Sciences) , 2021, 65 (1) .

[56] Li Zengpeng, Wang Ding, Morais E. Quantum-safe round-optimal password authentication for mobile devices [J]. IEEE Transactions on Dependable and Secure Computing, 2020: 1-1.

[57] Sheikh M S, Liang Jun, Wang Wensong. A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs) [J]. Sensors (Basel) , 2019, 19 (16): 3589.

[58] Ahmad F, Adnane A, Franqueira V N L, *et al.* Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of

chinaXiv:202205.00140v1

ChinaXiv合作期刊

Attackers'Strategies [J]. Sensors (Basel) , 2018, 18 (11): 4040.
[59] Sbai O, Elboukhari M. A simulation analysis of MANET's link-spoofing and replay attacks with ns-3 [C/OL]/ Proc of the 4th International Conference on Smart City Applications, 2020. http://doi. org. 2019: 1-5. 10. 1145/3368756. 3369049.
[60] Pougajendy J, Parthiban A R K. CDAI: a novel collaborative detection approach for impersonation attacks in vehicular ad‑hoc networks [J]. Security and Communication Networks, 2016, 9 (18): 5547-5562.
[61] Peng Tao, Liu Qin, Wang Guojun, *et al.* Multidimensional privacy preservation in location-based services [J]. Future Generation Computer Systems, 2018, 93: 312-326.
[62] Lai Chengzhe, Zheng Dong, Zhao Qinglan, *et al.* SEGM: A secure group management framework in integrated VANET-cellular networks [J]. Vehicular Communications, 2018, 11 (January 2018): 33-45.
[63] Gao Feng, He Jingsha, Zhang Feng. Method for identify service providers of user privacy information disclosure [J]. Journal on Communications, 2011, 32 (9A): 239-245.
[64] Li Feng, Zhang Wenzheng, Hu Jianyong, *et al.* Review of GuessandDetermine Attack on Stream Ciphers [J]. Communications Technology, 2018, 51 (10): 2443-2448.
[65] Yao Yuwei, Zhang Xinpeng, Wu Hanzhou, *et al.* A Novel Location Privacy Protection Algorithm for Social Discovery Application [J]. IETE Technical Review, 2020, 38 (1): 82-92.
[66] Benarous L, Kadri B. Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles [J]. Peer-to-Peer Networking and Applications, 2021, 15 (1): 461-472.
[67] Finlayson S G, Bowers J D, Ito J, *et al.* Adversarial attacks on medical machine learning [J]. Science, 2019, 363 (6433): 1287-1289.
[68] Kazuo S, Tetsu I. Quantum Attacks on Sum of Even-Mansour Pseudorandom Functions [J]. Information Processing Letters, 2022, 173 (January 2022): 106172.
[69] Dwork C, McSherry F, Nissim K, *et al.* Calibrating Noise to Sensitivity in Private Data Analysis [C]// Proc of the Third conference on Theory of Cryptography, 2006.
[70] McSherry F, Talwar K. Mechanism Design via Differential Privacy [C/OL]/ Proc of the 48th Annual IEEE Symposium on Foundations of Computer Science, 2007, http://doi. org. 2007: 94-103. 10. 1109/focs. 2007. 4389483.
[71] Abbey C K, Clarkson E, Barrett H H, *et al.* A method for approximating the density of maximum-likelihood and maximum a posteriori estimates under a Gaussian noise model [J]. Medical Image Analysis, 1998, 2 (4): 395-403.
[72] Cynthia D, Aaron R. The Algorithmic Foundations of Differential Privacy [J]. Foundations and Trends in Thcoretical Computer Scicnce, 2014, 9 (3-4): 211-407.
[73] Zhu Tianqing, Li Gang, Zhou Wanlei, *et al.* Diffcrential privacy and applications [J]. Advances in Information Security, 2017: 69.
[74] Xiong Xingxing, Liu Shubo, Li Dan, *et al.* A Comprehensive Survey on Local Differential Privacy [J]. Hindawi Security and Communication Networks, 2020, 2020: 8829523.
[75] Han Wenxi, Cheng Mingzhu, Lei Min, *et al.* Privacy Protection Algorithm For The Internet Of Vehicles Based On Local Differential Privacy And Game Model [J]. Computers, Materials & Continua, 2020, 64 (2): 1025-1038.
[76] Xiao Yonghui, Xiong Li. Protecting Locations with Differential Privacy under Temporal Correlations [C]// Proc of the 22nd ACM Conference on Computer and Communications Security. 2015: 1298-1309.
[77] Chen Rui, Li Haoran, Qin A K, *et al.* Private spatial data aggregation in the local setting [C/OL]/ Proc of the 32nd IEEE International Conference on Data Engineering, 2016. http://doi. org. 2016. 10. 1109/ICDE. 2016. 7498248.
[78] 霍峥，张坤，贺萍，等. 满足本地化差分隐私的众包位置数据采集 [J]. 计算机应用, 2019, 39 (3): 763-768. (Huo Zheng, Zhang Kun, He Ping, *et al.* Crowdsourcing location data acquisition to satisfy the local differential privacy [J]. Journal of Computer Applications, 2019, 39 (3): 763-768.)
[79] Jiang Tao, Wang Helen J, Hu Yihchun. Preserving location privacy in wireless LANs [C]// Proc of the 5th International Conference on Mobile systems, applications and services. 2007: 246-257.
[80] Arana O, Garcia F, Gomez J. Analysis of the effectiveness of transmission power control as a location privacy technique [J]. Computer Networks, 2019, 163 (C): 106880.
[81] Abughazalah S, Markantonakis K, Mayes K. Secure Improved Cloud-Based RFID Authentication Protocol [J]. Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, 2015: 147-164.
[82] Xiao Hannan, Alshehri A A, Christianson B. A Cloud-Based RFID Authentication Protocol with Insecure Communication Channels [J]. IEEE Trustcom 2016, 2016: 332-339.
[83] Fan Kai, Kang Junbin, Zhu Shanshan, *et al.* PermutationMatrix Encryption Based Ultralightweight Secure RFID Scheme in Internet of Vehicles [J]. sensors (Basel) , 2019, 19 (152) .
[84] Zhang Qikun, Li Yongjiao, Wang Ruifang, *et al.* Blockchain-based asymmetric group key agreement protocol for internet of vehicles [J]. Computers & Electrical Engineering, 2020, 86: 106713.
[85] Sweeney L. k-Anonymity: A Model for Protecting Privacy [J]. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10 (5): 557-570.
[86] Machanavajjhala A, Kifer D, Gehrke J, *et al.* L-diversity: Privacy beyond kanonymity [J]. ACM Transactions on Knowledge Discovery from Data, 2007, 1 (1): 3.
[87] Li Ninghui, Li Tiancheng, Venkatasubramanian S. t-Closeness: privacy beyond k-Anonymity and l-diversity [C/OL]/ Proc of the 23rd IEEE International Conference on Data Engineering, 2007. http://doi. org. 2007: 106–15. 10. 1109/ICDE. 2007. 367856.
[88] Woo H, Lee M. A hierarchical location service architecture for VANET with aggregated location update [J]. Computer Communications, 2018, 125: 38-55.
[89] Yang Min, Feng Yong, Fu Xiaodong, *et al.* Location privacy preserving scheme based on dynamic pseudonym swap zone for Internet of Vehicles [J]. International Journal of Distributed Sensor Networks, 2019, 15 (7): 155014771986550.
[90] Xu Xianyun, Chen Huifang, Xie Lei. A Location Privacy Preservation Method Based on Dummy Locations in Internet of Vehicles [J]. Applied Sciences, 2021, 11 (10): 4594.
[91] Zhou Lu, Du Suguo, Zhu Haojin, *et al.* Location Privacy in Usage-Based Automotive Insurance: Attacks and Countermeasures [J]. IEEE Transactions on Information Forensics and Security, 2019, 14 (1): 196-211.
[92] An Dou, Yang Qingyu, Yu Wei, *et al.* LoPrO: Location Privacy-preserving Online auction scheme for electric vehicles joint bidding and charging [J]. Future Generation Computer Systems, 2020, 107: 394-407.
[93] Shen Xiaoying, Wang Licheng, Pei Qingqi, *et al.* Location privacy-preserving in online taxi-hailing services [J]. Peer-to-Peer Networking and Applications, 2020, 14 (1): 69-81.
[94] Xiong Ping, Li Guirong, Ren Wei, *et al.* LOPO: a location privacy

chinaXiv:202205.00140v1

ChinaXiv合作期刊

preserving path optimization scheme for spatial crowdsourcing [J]. Journal of Ambient Intelligence and Humanized Computing, 2021: 1-16.
[95] Chen Biwen, Wu Libing, Wang Huaqun, *et al.* A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks [J]. IEEE Transactions on Vehicular Technology, 2020, 69 (6): 5813-5825.
[96] Xiong Jinbo, Ma Rong, Chen Lei, *et al.* A Personalized Privacy Protection Framework for Mobile Crowdsensing in IIoT [J]. IEEE Transactions on Industrial Informatics, 2020, 16 (6): 4231-4241.
[97] Gai Keke, Qiu Meikang, Zhao Hui. Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing [J]. IEEE Transactions on Big Data, 2017, 7 (4): 678-688.
[98] Wang Yi. 2021 Global Multi industry major network security events [R]. Information security and communication confidentiality. Journal of information security and communication confidentiality. 2021. https://www. 163. com/dy/article/GQG818ER0552NPC3. html.
[99] Jin Hongyu, Papadimitratos P. Resilient Privacy Protection for Location-Based Services through Decentralization [J]. ACM Transactions on Privacy and Security, 2019, 22 (4) .
[100] [100] Cui Yuanbo, Gao Fei, Li Wenmin, *et al.* Cache-Based Privacy Preserving Solution for Location and Content Protection in Location-Based Services [J]. Sensors (Basel) , 2020, 20 (16): 4651.
[101] [101] 崔杰，陈学峰，张静，等. 基于公交车缓存的车联网位置隐私保护方案 [J]. 通信学报，2021, 42 (7): 151-161. (Cui Jie, Chen Xuefeng, Zhang Jing, *et al.* Bus cache-based location privacy protection scheme in the Internet of vehicles [J]. Journal on Communications, 2021, 42 (7): 151-161.)
[102] [102] 李方伟，张海波，王子心. 车联网中基于 MEC 的 V2X 协同缓存和资源分配 [J]. 通信学报，2021, 42 (2): 27-36. (Li Fangwei, Zhang Haibo, Wang Zixin. V2X collaborative caching and resource allocation in MEC-based IoV [J]. Journal on Communications, 2021, 42 (2): 27-36.)
[103] [103] Wright C S. Bitcoin: A Peer-to-Peer Electronic Cash System [J]. Social Science Electronic Publishing, 2008.
[104] [104] Zhang Lei. Key management scheme for secure channel establishment in fog computing [J]. IEEE Transactions on Cloud Computing, 2019, 9 (3): 1117-1128.
[105] [105] Zhang Lei, Luo Mingxing, Li Jiangtao, *et al.* Blockchain based secure data sharing system for Internet of vehicles: A position paper [J]. Vehicular Communications, 2019, 16: 85-93.
[106] [106] Chen Yinru, Sha Jinrui, Zhou Zhihong. IOV Privacy Protection System Based on Double-Layered Chains [J]. Wireless Communications and Mobile Computing, 2019, 2019: 3013562.
[107] [107] Dwivedi S K, Amin R, Vollala S. Blockchain-Based Secured IPFS-Enable Event Storage Technique With Authentication Protocol in VANET [J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8 (12): 1913-1922.
[108] [108] Benet J. IPFS-Content Addressed, Versioned, P2P File System. [J]. IEICE Transactions on Fundamentals of Electronics, 2014, abs/1407. 3561.
[109] [109] Wang Jia, Li Jianqiang, Wang Huihui, *et al.* Dynamic Scalable Elliptic Curve Cryptographic Scheme and Its Application to In-Vehicle Security [J]. IEEE Internet of Things Journal, 2019, 6 (4): 5892-5901.
[110] [110] Nahri M, Boulmakoul A, Karim L, *et al.* IoV distributed architecture for real-time traffic data analytics [J]. Procedia Computer Science, 2018, 130 (2018): 480–487.
[111] [111] Wang Wenjie, Luo Tao, Kang Hongxia. A Local Information Sensing-Based Broadcast Scheme for Disseminating Emergency Safety Messages in IoV [J]. Mobile Information Systems, 2019, 2019: 8278904.
[112] [112] Wang Tian, Cao Zhihan, Wang Shuo, *et al.* Privacy-Enhanced Data Collection Based on Deep Learning for Internet of Vehicles [J]. IEEE Transactions on Industrial Informatics, 2020, 16 (10): 6663-6672.
[113] [113] Pang Meiyu, Wang Li, Fang Ningsheng. A collaborative scheduling strategy for IoV computing resources considering location privacy protection in mobile edge computing environment [J]. Journal of Cloud Computing, 2020, 9 (1) .
[114] [114] Singh P K, Singh R, Nandi S K, *et al.* Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract [J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22 (6): 3616-3630.
[115] [115] Deb P K, Roy C, Roy A, *et al.* DEFT: Decentralized Multiuser Computation Offloading in a Fog-Enabled IoV Environment [J]. IEEE Transactions on Vehicular Technology, 2020, 69 (12): 15978-15987.
[116] [116] Zhao Yanan, Wang Yunpeng, Wang Pengcheng, *et al.* PBTM: A Privacy-Preserving Announcement Protocol With Blockchain-Based Trust Management for IoV [J]. IEEE Systems Journal, 2020, 99: 1-10.
[117] [117] Tufail A, Namoun A, Ali A. Moisture Computing-Based Internet of Vehicles (IoV) Architecture for Smart Cities [J]. Sensors (Basel) , 2021, 21 (11): 3785.
[118] [118] Baruah B, Dhal S. A secure road condition monitoring scheme in cloud based VANET [J]. Computer Communications, 2021, 174: 131-142.
[119] [119] Firdaus M, Rahmadika S, Rhee K H. Decentralized Trusted Data Sharing Management on Internet of Vehicle Edge Computing (IoVEC) Networks Using Consortium Blockchain [J]. Sensors (Basel) , 2021, 21 (7) .
[120] [120] Campanile L, Iacono M, Marulli F, *et al.* Designing a GDPR compliant blockchain-based IoV distributed information tracking system [J]. Information Processing & Management, 2021, 58 (3): 102511.
[121] [121] Wang Shupeng, Sun Shouming, Wang Xiaojie, *et al.* Secure Crowdsensing in 5G Internet of Vehicles: When Deep Reinforcement Learning Meets Blockchain [J]. IEEE Consumer Electronics Magazine, 2021, 10 (5): 72-81.
[122] [122] Xu Xiaolong, Huang Qihe, Zhu Haibin, *et al.* Secure Service Offloading for Internet of Vehicles in SDN-Enabled Mobile Edge Computing [J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22 (6): 3720-3729.
[123] [123] 玄世昌，汤浩，杨武. 基于信誉积分的路况信息共享中共谋攻击节点检测方法 [J]. 通信学报，2021, 42 (4): 159-168. (Xuan Shichang, Tang Hao, Yang Wu. Method for detecting collusion attack node in road condition information sharing based on reputation point [J]. Journal on Communications, 2021, 42 (4): 159-168.)
[124] [124] Raja Sekhar K, Ravi Chandra T S, Pooja S, *et al.* Light weight security protocol for communications in vehicular networks [J]. Wireless Networks, 2016, 22 (4): 1343-1353.
[125] [125] Liu Yanbing, Wang Yuhang, Chang Guanghui. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm [J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18 (10): 2740-2749.
[126] [126] Kang Jiawen, Yu Rong, Huang Xumin, *et al.* Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19 (8): 2627-2637.
[127] [127] Pournaghi S M, Zahednejad B, Bayat M, *et al.* NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET [J]. Computer Networks, 2018, 134: 78-92.
chinaXiv:202205.00140v1

ChinaXiv合作期刊

[128] [128] Wang Xiaoliang, Zeng Pengjie, Patterson N, *et al.* An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology [J]. IEEE Access, 2019, 7: 45061-45072.

[129] [129] Li Jiliang, Ji Yusheng, Choo K K R, *et al.* CL-CPPA: Certificate-Less Conditional Privacy-Preserving Authentication Protocol for the Internet of Vehicles [J]. IEEE Internet of Things Journal, 2019, 6 (6): 10332-10343.

[130] [130] Fan Kai, Jiang Wei, Luo Qi, *et al.* Cloud-based RFID mutual authentication scheme for efficient privacy preserving in IoV [J]. Journal of the Franklin Institute, 2021, 358 (1): 193-209.

[131] [131] 崔永泉，曹玲，张小宇，等. 格基环签名的车联网隐私保护 [J]. 计算机学报，2019, 42 (5): 981-992. (Cui Yongquan, Cao Ling, Zhang Xiaoyu, *et al.* Ring Signature Based on Lattice and VANET Privacy Preservation [J]. Chinese journal of computers, 2019, 42 (5): 981-992.)

[132] [132] Junejo M H, Ab Rahman A A H, Shaikh R A, *et al.* A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks [J]. Scientific Programming, 2020, 2020: 8831611.

[133] [133] Su Tianhong, Shao Sujie, Guo Shaoyong, *et al.* Blockchain-Based Internet of Vehicles Privacy Protection System [J]. Wireless Communications and Mobile Computing, 2020, 2020: 8870438.

[134] [134] Song Liangjun, Sun Gang, Yu Hongfang, *et al.* FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles [J]. IEEE transactions on vehicular technology, 2020, 69 (5): 5403-5415.

[135] [135] Cui Jie, Wang Yali, Zhang Jing, *et al.* Full Session Key Agreement Scheme Based on Chaotic Map in Vehicular Ad Hoc Networks [J]. IEEE Transactions on Vehicular Technology, 2020, 69 (8): 8914-8924.

[136] [136] Memon I, Memon H, Arain Q A. Pseudonym Changing Strategy with Mix Zones Based Authentication Protocol for Location Privacy in Road Networks [J]. Wireless Personal Communications, 2020, 116 (4): 3309-3329.

[137] [137] 张文芳，雷丽婷，王小敏，等. 面向云服务的安全高效无证书聚合签名车联网认证密钥协商协议 [J]. 电子学报，2020, 48 (9): 0372-2112 (020) 09-1814-10. (Zhang Wenfang, Lei Liting, Wang Xiaomin, *et al.* Secure and Efficient Authentication and Key Agreement Protocol Using Certificateless Aggregate Signature for Cloud Service Oriented VANET [J]. Acta Electronica Sinica, 2020, 48 (9): 0372-2112 (020) 09-1814-10.)

[138] [138] Akhter A F M S, Ahmed M, Shah A F M S, *et al.* A Blockchain-Based Authentication Protocol for Cooperative Vehicular Ad Hoc Network [J]. Sensors (Basel) , 2021, 21 (4): 1273.

[139] [139] Meng Xiangwei, Xu Jinbo, Liang Wei, *et al.* A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for internet of vehicles [J]. Computers & Electrical Engineering, 2021, 95: 107431.

[140] [140] Miao Junfeng, Wang Zhaoshun, Miao Xue, *et al.* A Secure and Efficient Lightweight Vehicle Group Authentication Protocol in 5G Networks [J]. Wireless Communications and Mobile Computing, 2021, 2021: 4079092.

[141] [141] Zhang Mingyue, Zhou Junlong, Zhang Gongxuan, *et al.* EC-BAAS: Elliptic curve-based batch anonymous authentication scheme for Internet of Vehicles [J]. Journal of Systems Architecture, 2021, 117: 102161.

[142] [142] Al-Marshoud M S, Al-Bayatti A H, Kiraz M S. Improved Chaff-Based CMIX for Solving Location Privacy Issues in VANETs [J]. Electronics, 2021, 10 (11): 1302.

[143] [143] Ullah I, Shah M A, Khan A, *et al.* Virtual Pseudonym-Changing and Dynamic Grouping Policy for Privacy Preservation in VANETs [J]. Sensors (Basel) , 2021, 21 (9) .

[144] [144] 张文波，黄文华，冯景瑜. 基于无证书签密的车联社会网络安全通信机制 [J]. 通信学报，2021, 42 (7): 129-136. (Zhang Wenbo, Huang Wenhua, Feng Jingyu. Secure communication mechanism for VSN based on certificateless signcryption [J]. Journal on Communications, 2021, 42 (7): 129-136.)

[145] [145] 韩牟，杨晨，华蕾，等. 面向移动边缘计算车联网中车辆假名管理方案 [J]. 计算机研究与发展，2021: 1-15. (Han Mu, Yang Chen, Hua Lei, *et al.* Vehicle Pseudonym Management Scheme in Internet of Vehicles for Mobile Edge Computing [J]. Journal of Computer Research and Development, 2021: 1-15.)

[146] [146] 侯慧莹，廉欢欢，赵运磊. 面向自动驾驶的高效可追踪的车联网匿名通信方案 [J]. 计算机研究与发展，2021: 1-21. (Hou Huiying, Lian Huanhuan, Zhao Yunlei. An Efficient and Traceable Anonymous VANET Communication Scheme for Autonomous Driving [J]. Journal of Computer Research and Development, 2021: 1-21.)

[147] [147] Gupta D S, Ray S, Singh T, *et al.* Post-quantum lightweight identity-based two-party authenticated key exchange protocol for Internet of Vehicles with probable security [J]. Computer Communications, 2022, 181: 69-79.

[148] [148] Zhou Lu, Yu Le, Du Suguo, *et al.* Achieving Differentially Private Location Privacy in Edge-Assistant Connected Vehicles [J]. IEEE Internet of Things Journal, 2019, 6 (3): 4472-4481.

[149] [149] Aoki S, Sezaki K, Yuan N J, *et al.* BusBeat: Early Event Detection with Real-Time Bus GPS Trajectories [J]. IEEE Transactions on Big Data, 2021, 7 (2): 371-382.

[150] [150] Liao Dan, Li Hui, Sun Gang, *et al.* Location and trajectory privacy preservation in 5G-Enabled vehicle social network services [J]. Journal of Network and Computer Applications, 2018, 110: 108-118.

[151] [151] Park Y, Sur C, Noh S W, *et al.* Self-Controllable Secure Location Sharing for Trajectory-Based Message Delivery on Cloud-Assisted VANETs [J]. Sensors (Basel) , 2018, 18 (7) .

[152] [152] Cui Jie, Wen Jingyu, Han Shunshun, *et al.* Efficient Privacy-Preserving Scheme for Real-Time Location Data in Vehicular Ad-Hoc Network [J]. IEEE Internet of Things Journal, 2019, 5 (5): 3491-3498.

[153] [153] Liu Shushu, Liu An, Yan Zheng, *et al.* Efficient LBS queries with mutual privacy preservation in IoV [J]. Vehicular Communications, 2019, 16: 62-71.

[154] [154] Ma Zhuo, Zhang Tian, Liu Ximeng, *et al.* Real-Time Privacy-Preserving Data Release Over Vehicle Trajectory [J]. IEEE Transactions on Vehicular Technology, 2019, 68 (8): 8091-8102.

[155] [155] Yadav V K, Verma S, Venkatesan S. Efficient and Secure Location-Based Services Scheme in VANET [J]. IEEE Transactions on Vehicular Technology, 2020, 69 (11): 13567-13578.

[156] [156] Chen Hua, Xiong Chen, Xie Jiameng, *et al.* Privacy Protection Method for Vehicle Trajectory Based on VLPR Data [J]. Journal of Advanced Transportation, 2020, 2020: 6026140.

[157] [157] Ye Xin, Zhou Jin, Li Yuedi, *et al.* A location privacy protection scheme for convoy driving in autonomous driving era [J]. Peer-to-Peer Networking and Applications, 2021, 14 (3): 1388-1400.

[158] [158] Zhu Qingfeng, Ji Sai, Shen Jian, *et al.* Privacy-Preserving Smart Road-Pricing System with Trustworthiness Evaluation in VANETs [J]. Sensors (Basel) , 2021, 21 (11) .

[159] [159] Choi S, Kim J, Yeo H. TrajGAIL: Generating urban vehicle trajectories using generative adversarial imitation learning [J]. Transportation Research Part C: Emerging Technologies, 2021, 128:

chinaXiv:202205.00140v1

ChinaXiv合作期刊

103091.

[160] [160] Babaghayou M, Labraoui N, Maglaras L, *et al.* WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles [J]. Sensors (Basel) , 2021, 21 (7): 2443.

[161] [161] Gopal L, Singh A K, Shanmugam V. Power Estimation in Mobile Communication Systems [J]. Computer and Information Science, 2008, 1 (3): 88-94.

chinaXiv:202205.00140v1